4-2013

Information security as a credence good

Ping Fan KE
Singapore Management University, pfke@smu.edu.sg

Kai-Lung HUI

Wei Thoo YUE

Information Security as a Credence Good

Ping Fan Ke[1], Kai-Lung Hui[1], and Wei T. Yue[2]

[1] Hong Kong University of Science and Technology
pfke@ust.hk, klhui@ust.hk
[2] City University of Hong Kong
wei.t.yue@cityu.edu.hk

Abstract. With increasing use of information systems, many organizations are outsourcing information security protection to a managed security service provider (MSSP). However, diagnosing the risk of an information system requires special expertise, which could be costly and difficult to acquire. The MSSP may exploit their professional advantage and provide fraudulent diagnosis of clients' vulnerabilities. Such an incentive to mis-represent clients' risks is often called the *credence goods* problem in the economics literature[3]. Although different mechanisms have been introduced to tackle the credence goods problem, in the information security outsourcing context, such mechanisms may not work well with the presence of *system interdependency risks*[6], which are introduced by inter-connecting multiple clients' systems by the MSSP. In particular, we find that allowing clients to seek alternative diagnosis of their vulnerabilities may not remove the MSSP's fraudulent behaviors. We shall explore alternative ways to solve the credence goods problem in the information security outsourcing context.

Keywords: Information security outsourcing, credence good, interdependency risks

1 Introduction

Enhancing the security of information systems has become an important task for organizations. An accurate risk assessment is often important in implementing a cost-efficient security protection. By knowing the actual risk level, an organization can procure the appropriate level of security protection.[3] However, it is not easy to accurately diagnose the risk of an information system, especially for organizations without proper security expertise. Therefore, many organizations would prefer to outsource their security protection to a managed security service provider (MSSP). Yet, the information asymmetry between the MSSP and his clients introduces an incentive for the MSSP to cheat his clients, which could

[3] An excessively high security protection could lead to wastage of resources and poor usability. Similarly, sub-standard security protection could expose the organization to excessive risks and losses.

subsequently lead to fraudulent behaviors.[4][5][4] In this study, we investigate such an incentive and discuss the implications for practices of security protection. We also study the challenges brought by system interdependency, which is a key feature of information security outsourcing that introduces new risks to the clients.[2][6]

Our model is founded on contract theory in economics, which studies how the MSSP and his clients behave based on their incentives.[1] While the prior literature in credence goods studies mechanisms to prevent *inefficient treatment*[3][4][5], our study focuses on *fraudulent diagnosis* and how clients can obtain their true risk level from the MSSP's diagnosis. In particular, we shall discuss how the MSSP decides his pricing mechanism and how it variously relates to his incentive to provide honest/dishonest diagnosis.

Section 2 presents our basic model. We start by showing that the MSSP will always charge one price to all clients of different risks, and hence his diagnosis is un-informative. Then, we introduce the self-diagnosis option to the clients and show that it incentivizes the MSSP to provide truthful diagnosis. Section 3 discusses the impact of introducing system interdependency risk. In particular, we show that in the presence of system interdependency risks self-diagnosis is insufficient to rectify the MSSP's incentive to hide the clients' risks.

2 Basic Model

We make the following assumptions in the basic model: [A1] There are n clients and one managed security service provider (MSSP). Each client values her system at v. [A2] Each client's system face a particular risk $\omega \in \{h, l\}$ decided by the nature. The probability of being high risk is r, and the probability of being low risk is $1 - r$. [A3] A high risk system will be attacked by a hacker with probability $a_h \in (0, 1)$. A low risk system will be attacked with probability $a_l \in (0, 1)$, $a_h > a_l$. [A4] The clients do not know their risk levels. The MSSP can accurately diagnose clients' risk levels. [A5] The unit cost of security protection quality q, which represents the probability of deterring an attack, is c_k for clients and c_s for MSSP, $c_k > c_s$. [A6] v, r, a_h, a_l, c_k, c_s are public information. [A7] $a_h v < c_s$. [A8] The clients cannot verify the MSSP's effort in security protection (i.e., there is no verifiability).

Assumption A7 implies complete security protection is cost-inefficient, and so it avoids a corner solution with $q^* = 1$. Assumption A8 implies that the MSSP will choose the security quality independent of the protection fee he charges.

The game begins with nature chooses clients' risk level, and the MSSP chooses capacity m and publishes contract information such as price p. After that, a client will decide whether to consult the MSSP. If not, she will directly choose protection quality in-house. Otherwise, she will visit the MSSP and receive a diagnosis. Based on the diagnosis result and offered price, the client will decide whether to accept the service. The MSSP will choose protection quality

[4] For example, the MSSP may exaggerate his clients' risks and over-charge them without working hard to protect them.

if she accept, or she will just choose protection quality in-house otherwise. After the protection quality is decided, the hacker launches attacks and outcomes are realized.

A client who does nothing in security protection will have expected utility $u_0 = (1 - \bar{a})\, v$, where $\bar{a} = ra_h + (1 - r)\, a_l$ is the expected attack rate. Suppose that a client has decided to develop security protection in-house. Her expected utility would be

$$u_k = [1 - \bar{a}\,(1 - q_k)]\, v - \frac{1}{2} c_k q_k^2, \tag{1}$$

where q_k is the security quality from in-house development. Differentiating u_k with respect to q_k, the optimal quality is $q_k^* = \frac{\bar{a}v}{c_k}$. Therefore, the expected utility of the client with in-house development is

$$u_k^* = (1 - \bar{a})\, v + \frac{1}{2} \frac{(\bar{a}v)^2}{c_k}, \tag{2}$$

which is greater than the expected utility of not protecting the system, i.e. $u_k^* > u_0$. Hence, u_k^* is the client's reservation utility.

To attract clients to use his service, the MSSP has to introduce a compensation term ("Liability") $\beta \in (0, 1]$ in the contract. If a client is attacked under the MSSP's protection and loses v, then the MSSP has to compensate her by βv. Without such compensation, by assumption A8, the MSSP can always minimize his cost by providing $q_s = 0$, which is undesirable to the clients.

2.1 One Price Solves All

We first consider the case where the MSSP charges a single price p on security protection to all clients. A client's expected utility of outsourcing to the MSSP would be

$$u_s = r\,[1 - a_h\,(1 - \beta)\,(1 - q_{s,h})]\, v + (1 - r)\,[1 - a_l\,(1 - \beta)\,(1 - q_{s,l})]\, v - p, \tag{3}$$

and the MSSP's expected profit would be

$$\pi = r\left[p - a_h\,(1 - q_{s,h})\,\beta v - \frac{1}{2} c_s q_{s,h}^2\right] + (1 - r)\left[p - a_l\,(1 - q_{s,l})\,\beta v - \frac{1}{2} c_s q_{s,l}^2\right]. \tag{4}$$

Differentiating π with respect to $q_{s,h}$ and $q_{s,l}$, the optimal quality is $q_{s,h}^* = \frac{a_h \beta v}{c_s}$ and $q_{s,l}^* = \frac{a_l \beta v}{c_s}$. By backward induction, the client's expected utility of outsourcing becomes

$$u_s = (1 - \bar{a})\, v + \bar{a}\beta v + \frac{\left(\bar{a}^2 + \sigma_a^2\right) v^2}{c_s} \beta\,(1 - \beta) - p, \tag{5}$$

where $\sigma_a^2 = r\,(1 - r)\,(a_h - a_l)^2$ is the variance of the attack rate. Substituting $q_{s,h}^*$ and $q_{s,l}^*$ into (4), the MSSP's profit maximization problem becomes:

$$\max_{p,\beta} \left[p - \bar{a}\beta v + \frac{1}{2} \frac{\left(\bar{a}^2 + \sigma_a^2\right) (\beta v)^2}{c_s}\right]$$

$$\text{s.t. } p \leq \bar{a}\beta v + v^2 \left[\frac{\beta\left(1-\beta\right)\left(\bar{a}^2+\sigma_a^2\right)}{c_s} - \frac{1}{2}\frac{\bar{a}^2}{c_k} \right].$$

The price constraint ensures that the clients are not worse off after using the MSSP's service, i.e. $u_s \geq u_k^*$. The optimal solution is $\beta^* = 1$, $p^* = \bar{a}v - \frac{1}{2}\frac{(\bar{a}v)^2}{c_k}$, and $\pi^* = \frac{v^2}{2}\left(\frac{\bar{a}^2+\sigma_a^2}{c_s} - \frac{\bar{a}^2}{c_k}\right) > 0$.

Will the MSSP price discriminate, i.e., offer p_h to high risk clients and p_l to low risk clients? It turns out that he will not. If he sets the prices honestly, the clients will learn their own risk levels from the MSSP's diagnosis and pricing. This will help the clients select the proper q_k with respect to their risk levels, which would increase their reservation utility and so decrease the MSSP's profit. On the other hand, if the MSSP "cheats" the clients on pricing, then they could always maximize their utility by only accepting a low price, $p_l \leq p^*$.

From the above reasoning, we propose that the MSSP will prefer to offer a single price contract in the information security outsourcing market:

Proposition 1. In information security outsourcing, setting a single price contract with liability term, which does not reveal any risk information of the clients, is optimal for the MSSP.

Note that the low risk clients are worse off because they will be subsidizing the high risk clients. Therefore, the MSSP will tend to exaggerate clients' risk to encourage them to use his service. Once the clients recognize this fact, they will probably ignore the MSSP's recommendation and protect their own system using the average quality. This results in either over-protected for low risk clients or under-protected for high risk clients, which makes the system less usable.

We next consider the case when the clients can seek alternative diagnosis (we call this "self-diagnosis").

2.2 Self-Diagnosis

With self-diagnosis, we assume that the clients can pay d_k to a third-party consultant to reveal her risk. After self-diagnosis, the clients can treat themselves using the corresponding quality, i.e. $q_{k,h}^* = \frac{a_h v}{c_k}$ and $q_{k,l}^* = \frac{a_l v}{c_k}$. The reservation utility of a client with risk level ω after self-diagnosis and self-treatment will be

$$u_{k,\omega}^{d*} = \left(1-a_\omega\right)v + \frac{1}{2}\frac{\left(a_\omega v\right)^2}{c_k} - d_k. \tag{6}$$

Further, the client will choose between in-house protection and outsourcing, depending on which option gives more utility, after self-diagnosis. Therefore, the minimum expected utility of a client after self-diagnosis would be

$$u_k^{d*} = \left(1-\bar{a}\right)v + \frac{1}{2}\frac{\left(\bar{a}v\right)^2}{c_k} + \frac{1}{2}\frac{\left(\sigma_a v\right)^2}{c_k} - d_k. \tag{7}$$

If $d_k \leq \frac{1}{2}\frac{(\sigma_a v)^2}{c_k}$, then $u_k^{d*} \geq u_k^*$, which means that it is efficient for clients to seek self-diagnosis. We will assume that such a condition holds in the following analysis.

We first consider the case where the MSSP charges different prices for different types of clients. Suppose that the MSSP charges honestly, i.e., offering p_h to high risk clients and p_l to low risk clients. This situation is similar to serving two market segments with $r = 1$ and $r = 0$, which is both profitable. Therefore, he will serve both types of clients with the following profit maximization problem:

$$\max_{p_h,p_l,\beta} r\left[p_h - a_h\beta v + \frac{1}{2}\frac{(a_h\beta v)^2}{c_s}\right] + (1-r)\left[p_l - a_l\beta v + \frac{1}{2}\frac{(a_l\beta v)^2}{c_s}\right],$$

$$\text{s.t. } u_{s,h} \geq u_{k,h}^*,\ u_{s,l} \geq u_{k,l}^*.$$

The constraints show that the MSSP charges the clients honestly so that a client with a particular type of risk will not be worse off. The solution is $\beta^* = 1$, $p_h^* = a_h v - \frac{1}{2}\frac{(a_h v)^2}{c_k} > p_l^* = a_l v - \frac{1}{2}\frac{(a_l v)^2}{c_k}$, and $\pi^* = \frac{\left(\bar{a}^2+\sigma_a^2\right)v^2}{2}\left(\frac{1}{c_s} - \frac{1}{c_k}\right)$.

However, the MSSP has incentive to overcharge the low risk clients with p_h^*, which is the main reason that price discrimination is unsustainable in the case without self-diagnosis. A client will always accept p_l^* since it is beneficial for either type, and self-diagnose only when p_h^* is offered. By doing so, the clients can punish a dishonest MSSP by turning down the p_h^* offer and do in-house protection instead. Therefore, the MSSP will earn nothing if he overcharges the clients, and the clients know it.

We next consider the possibility of a mixed self-diagnosis strategy. To construct such a strategy, consider the profit of serving a low risk client with low price:

$$\pi_{l,p_l^*} = \frac{(a_l v)^2}{2}\left(\frac{1}{c_s} - \frac{1}{c_k}\right), \tag{8}$$

and the profit of serving a low risk client with a high price:

$$\pi_{l,p_h^*} = (1-\rho)\left[\frac{(a_l v)^2}{2}\left(\frac{1}{c_s} - \frac{1}{c_k}\right) + (a_h - a_l)\, v\left(1 - \frac{1}{2}\frac{a_h v}{c_k} - \frac{1}{2}\frac{a_l v}{c_k}\right)\right], \tag{9}$$

where ρ is the probability of self-diagnosis when a client was offered a high price ("Re-diagnosis Rate"). An effective mixed strategy should result in $\pi_{l,p_h^*} \leq \pi_{l,p_l^*}$, which gives rise to the re-diagnosis rate:

$$\rho \geq \frac{(a_h - a_l)\left(1 - \frac{1}{2}\frac{a_h v}{c_k} - \frac{1}{2}\frac{a_l v}{c_k}\right)}{(a_h - a_l)\left(1 - \frac{1}{2}\frac{a_h v}{c_k} - \frac{1}{2}\frac{a_l v}{c_k}\right) + a_l^2 v\left(\frac{1}{c_s} - \frac{1}{c_k}\right)}. \tag{10}$$

The client would maximize her utility by minimizing the re-diagnosis rate, and so the equality holds for (10) in equilibrium. This re-diagnosis rate removes the MSSP's incentive to cheat and supports the price discrimination equilibrium.

We now consider the case where the MSSP charges a single price p to all clients. If all client prefer to self-diagnose, then at least one type of clients would benefit from using the revealed risk information for in-house treatment. So, the MSSP can earn more by serving both types of clients with price discrimination. On the other hand, the clients would prefer to use the MSSP's service directly without self-diagnosis if and only if the MSSP charges them a low price. But, by doing so he will get sub-optimal profit because he is practically giving out surplus to high risk clients.

From the above discussion, the MSSP could earn more profit by price discrimination. Hence, the self-diagnosis option removes the MSSP's incentive to conceal risk information.

Proposition 2. With a cheap self-diagnosis option, the MSSP will truthfully reveal the clients' risk information.

When the MSSP's diagnosis result is verifiable at a low cost, clients can actually learn from the MSSP's recommendation. As a result, they can protect their own system according to their own risk, so that the systems are secured without losing usability. However, in reality, different systems are often interconnected to address users' need, which introduce new challenges. In the next section, we will examine how system interdependency risks affect the current situation.

3 System Interdependency Model

We add the following assumption to extend the basic model with system interdependency risks: [A9] A client who joined the MSSP's network will lose εv if at least one other system in the MSSP's network is compromised. The MSSP needs to compensate $\beta\varepsilon v$ to all affected clients who are not directly attacked.

Consider the MSSP's network with m clients. The probability of at least one system being attacked is

$$P_{X>0} = 1 - \prod_{i=1}^{m_h} \left[1 - a_h \left(1 - q_{s,h,i}\right)\right] \prod_{i=1}^{m_l} \left[1 - a_l \left(1 - q_{s,l,i}\right)\right], \tag{11}$$

where m_h is the number of high risk clients in the network, m_l is the number of low risk clients in the network, $m_h + m_l = m$. The loss of a client j with risk level ω will be $L_{\omega,j}v = a_\omega \left(1 - q_{s,\omega,j}\right)\left(1 - \varepsilon\right)v + \varepsilon v P_{X>0}$. Since the loss involves m-th order terms, to simplify the analysis, we approximate it by only retaining the first order terms:

$$\tilde{L_{\omega,j}} = a_\omega \left(1 - q_{s,\omega,j}\right)\left(1 - \varepsilon\right) + \varepsilon \left[\sum_{i=1}^{m_h} a_h \left(1 - q_{s,h,i}\right) + \sum_{i=1}^{m_l} a_l \left(1 - q_{s,l,i}\right)\right]. \tag{12}$$

3.1 Without Self-Diagnosis

Suppose that the MSSP charges p to all clients. The expected utility of client j who uses the MSSP's service would be

$$u_{s,j} = r\left[\left(1 - L_{h,j}\right)v + L_{h,j}\beta v - p\right] + \left(1 - r\right)\left[\left(1 - L_{l,j}\right)v + L_{l,j}\beta v - p\right], \tag{13}$$

and the MSSP's expected total profit would be

$$\pi = \sum_{i=1}^{m_h} \left(p - L_{h,i}\beta v - \frac{1}{2} c_s q_{s,h,i}^2 \right) + \sum_{i=1}^{m_l} \left(p - L_{l,i}\beta v - \frac{1}{2} c_s q_{s,l,i}^2 \right). \tag{14}$$

Differentiating π with respect to $q_{s,h,i}$ and $q_{s,l,i}$, the optimal quality is $q_{s,h,i}^* = \frac{T a_h \beta v}{c_s}$ and $q_{s,l,i}^* = \frac{T a_l \beta v}{c_s}$, where $T = 1 + \varepsilon (m-1)$ is the (amplified) risk factor due to system interdependency.

The expected utility of outsourcing the protection would then become

$$u_s = \left[1 - \bar{L} (1 - \beta) \right] v - p, \tag{15}$$

where $\bar{L} = T\bar{a} - \frac{T^2 \left(\bar{a}^2 + \sigma_a^2 \right) \beta v}{c_s}$ is the expected loss after outsourcing. Now, suppose that the MSSP is committed to serve a client after diagnosis, which means that he cannot freely choose m_h and m_l. In a network with m clients, the expected number of high risk clients would be $E[m_h] = rm$, and the expected number of low risk clients would be $E[m_l] = (1-r)m$. Therefore, the MSSP's profit maximization problem becomes

$$\max_{p,\beta,m} m \left[p - \bar{L}\beta v - \frac{1}{2} \frac{\left(\bar{a}^2 + \sigma_a^2 \right) (T\beta v)^2}{c_s} \right]$$

$$\text{s.t. } p \leq \left(\bar{a} - \bar{L} \right) v + \bar{L}\beta v - \frac{1}{2} \frac{(\bar{a}v)^2}{c_k}.$$

The solution is $\beta^* = 1$, $p^* = \bar{a}v - \frac{1}{2} \frac{(\bar{a}v)^2}{c_k}$, and the number of clients served by the MSSP satisfies the following equation: $m^* = \frac{1}{2} + \frac{E[aq_s^*]v - \frac{1}{2} c_s E\left[q_s^{*2}\right] - \frac{1}{2} \frac{(\bar{a}v)^2}{c_k}}{2\varepsilon v (\bar{a} - E[aq_s^*])}$, where $E[aq_s^*] = r a_h q_{s,h}^* + (1-r) a_l q_{s,l}^*$ and $E\left[q_s^{*2}\right] = r q_{s,h}^{*2} + (1-r) q_{s,l}^{*2}$.

If the MSSP can freely choose m_h and m_l, when he will charge p^*, a low risk client who uses the MSSP's service will be subsidizing the high risk clients. Therefore, the optimal decision for the MSSP is to serve only the low risk clients in equilibrium, and get the subsidies as profit.

However, once the clients realize this, they will demand for a lower price since p^* is not a desirable price for low risk clients. Therefore, the MSSP can no longer charge p^* if he does not commit to serve the clients, which results in sub-optimal profits.

What if the MSSP sets different prices for different clients? Since the interdependency risk limits the MSSP's capacity, and serving a high risk client with p_h^* is more profitable compared with serving a low risk client with p_l^*, the MSSP will prefer to serve only the high risk clients. Specifically, the optimal decision for capacity satisfies $m_l^* = 0$ and $m_h^* = \frac{1}{2} + \frac{a_h v q_{s,h}^* - \frac{1}{2} c_s q_{s,h}^{*2} - \frac{1}{2} \frac{(a_h v)^2}{c_k}}{2\varepsilon a_h v \left(1 - q_{s,h}^* \right)}$. Therefore, the MSSP has great incentive to overcharge the low risk clients, since kicking out a low risk client is not a problem.[5] Hence, the MSSP always prefers to offer

[5] If a low risk client accepts p_h, the MSSP can earn even more since the required protection level and the interdependency risk brought by this client is lower.

a high price p_h, which means that posting two prices cannot be an equilibrium strategy.

Yet, clients will only accept a low price p_l, and they will suspect that they get overcharged when p_h is offered. These competing strategies cause the market to breakdown.

If the MSSP uses a mixed strategy and offers p_h and p_l sometimes, clients will only accept when p_l is offered, which result in sub-optimal profit compared with the case of using single price with service commitment.

From the above discussion, if the MSSP does not commit to serve every clients, then he will end up serving only one type of clients. This reveal the clients' risk information, and hence result in sub-optimal profit, or even market breakdown. Therefore, the MSSP will prefer to charge a single price and commit to serve every client, which leads to a similar outcome as Proposition 1.

3.2 With Self-Diagnosis

Continue from the above discussion, when the MSSP posts two prices, he is committed to serve any clients with p_h. However, with self-diagnosis, the clients can verify whether they really get overcharged. Hence, the clients who learn that they have a high risk from self-diagnosis will continue to use the MSSP's service.

The market will not breakdown and the MSSP's aggressive pricing strategy is actually "resurrected" by self-diagnosis. The MSSP has no incentive to deviate from this strategy, since offering $p_l < p_h$ will result in sub-optimal profit.

Therefore, even when self-diagnosis is feasible, the credence goods problem still remains when system interdependency is present.

Proposition 3. In the presence of system interdependency, when there are sufficient high risk clients in the market and the clients can cheaply self-diagnose, then the MSSP will always charge a single price p_h, and only high risk clients will use the MSSP's service. In other words, self-diagnosis will not dissuade the MSSP's from concealing the clients' risk information.

In this situation, low risk clients are rejected by the MSSP, so that they cannot enjoy a better protection. Even worse, every clients need to verify the MSSP's diagnosis, which results in duplication of diagnosis cost.

4 Final Remarks

The typical credence goods problem is often solved by introducing verifiability of the service provider's efforts. Here, we show that by introducing verifiability in the MSSP's diagnosis (which is done by self-diagnosis), the MSSP will truthfully reveal the clients' risks in the basic setting. However, when we introduce system interdependency risks into the model, the MSSP will have incentives to exaggerate clients' risks and offer a high price, which seems common in reality. This brings challenges to organizations that want to learn their risk level and avoid constantly over-paying for security protections. In future work we shall study alternative mechanisms that can tackle this challenge.

References

1. Akerlof, G.A.: The market for "lemons": Quality uncertainty and the market mechanism. The Quarterly Journal of Economics. 84(3), 488–500 (1970)
2. Anderson, R., Moore, T.: The economics of information security. Science. 314(5799), 610–613 (2006)
3. Dulleck, U., Kerschbamer, R.: On doctors, mechanics, and computer specialists: The economics of credence goods. Journal of Economic Literature. 44(1), 5–42 (2006)
4. Emons, W.: Credence goods and fraudulent experts. RAND Journal of Economics. 28(1), 107–119 (1997)
5. Fong, Y.: When do experts cheat and whom do they target? RAND Journal of Economics. 36(1), 113–130 (2005)
6. Kunreuther, H., Heal, G.: Interdependent security. Journal of Risk and Uncertainty. 26(2), 231–249 (2003)

Appendix: Proof of Propositions

Proof of Proposition 1

We first derive the equilibrium profit under single price contract. The Lagrange function of the profit maximization problem is

$$\Lambda = p - \bar{a}\beta v + \frac{\left(\bar{a}^2 + \sigma_a^2\right)(\beta v)^2}{2c_s} - \lambda\left\{p - \bar{a}\beta v - v^2\left[\frac{\beta(1-\beta)\left(\bar{a}^2+\sigma_a^2\right)}{c_s} - \frac{\bar{a}^2}{2c_k}\right]\right\} \tag{16}$$

where $\lambda \geq 0$. The first order conditions are:

$$\frac{\partial \Lambda}{\partial p} = 1 - \lambda = 0 \tag{17}$$

$$\frac{\partial \Lambda}{\partial \beta} = \frac{\left(\bar{a}^2+\sigma_a^2\right)v^2}{c_s}(\beta - 2\beta\lambda + \lambda) - \bar{a}v(1-\lambda) \tag{18}$$

and the Kuhn-Tucker condition is:

$$-\lambda\left\{p - \bar{a}\beta v - v^2\left[\frac{\beta(1-\beta)\left(\bar{a}^2+\sigma_a^2\right)}{c_s} - \frac{1}{2}\frac{\bar{a}^2}{c_k}\right]\right\} = 0 \tag{19}$$

Solving the above equations, we have $\lambda = 1$, $\beta^* = 1$, and $p^* = \bar{a}v - \frac{1}{2}\frac{(\bar{a}v)^2}{c_k}$. Substitute them back to (4) and (5) yields the client's expected utility and the MSSP's expected profit:

$$u_s^* = (1-\bar{a})v + \frac{1}{2}\frac{(\bar{a}v)^2}{c_k} = u_k^* \tag{20}$$

$$\pi^* = \frac{v^2}{2}\left(\frac{\bar{a}^2+\sigma_a^2}{c_s} - \frac{\bar{a}^2}{c_k}\right) \tag{21}$$

We then prove that price discrimination is sub-optimal. Suppose the MSSP charges two price honestly, then clients can infer their risk information and use it to decide in-house protection quality. The reservation utility of a client with risk level ω is

$$u_{k,\omega}^{**} = (1 - a_\omega)\, v + \frac{1}{2}\frac{(a_\omega v)^2}{c_k} \tag{22}$$

which can be obtained by considering a degenerated market with $r = 1$ and $r = 1$ on (2). Hence, the overall expected reservation utility of a client will be

$$u_k^{**} = (1 - \bar{a})\, v + \frac{1}{2}\frac{\left(\bar{a}^2 + \sigma_a^2\right) v^2}{c_k} \tag{23}$$

Since the overall reservation utility u_k^{**} is increased, and the total welfare between a client and the MSSP does not change, the MSSP's profit is decreased. Specifically, it becomes:

$$\pi^{**} = \frac{\left(\bar{a}^2 + \sigma_a^2\right) v^2}{2}\left(\frac{1}{c_s} - \frac{1}{c_k}\right) \tag{24}$$

By comparing (21), (22), (24) and (25), part of the MSSP's surplus $\frac{1}{2}\frac{(\sigma_a v)^2}{c_k}$ moves towards the client. Therefore, offering a single price is optimal for the MSSP.

Proof of Proposition 2

We first discuss the way to obtain the equilibrium profit, which is basically applying the result in Proposition 1. Consider the MSSP serves two different market with $r = 1$ and $r = 0$, and substitute them into the equilibrium profit from Proposition 1, i.e. (22). By taking the weighted average, we can obtain the equilibrium profit:

$$\pi^{*} = \frac{\left(\bar{a}^2 + \sigma_a^2\right) v^2}{2}\left(\frac{1}{c_s} - \frac{1}{c_k}\right) \tag{25}$$

We then show that the MSSP will not stick on offering a single price in the equilibrium. Firstly, it is trivial to see that if not all clients uses the MSSP's service, his profit will be sub-optimal and he can increase it by price discrimination. Secondly, If every clients uses the MSSP's service, the total welfare the MSSP and a client will be

$$W = r\left\{\left[1 - a_h\left(1 - q_{s,h}^{*}\right)\right] v - \frac{c_s q_{s,h}^{*2}}{2}\right\} + (1 - r)\left\{\left[1 - a_l\left(1 - q_{s,l}^{*}\right)\right] v - \frac{c_s q_{s,l}^{*2}}{2}\right\} \tag{26}$$

which is obtained by applying the MSSP's cost c_s into clients' problem. Note that the total welfare $W = u_s + \pi$ in this case. From previous analysis, the optimal quality for the MSSP will always be $q_{s,h}^{*} = \frac{a_h \beta v}{c_s}$ and $q_{s,l}^{*} = \frac{a_l \beta v}{c_s}$. Hence, (27) could be re-written as:

$$W = (1 - \bar{a})\, v + \left(\bar{a}^2 + \sigma_a^2\right) v^2 \left[\frac{\beta\,(2 - \beta)}{2c_s}\right] \tag{27}$$

A client will only use the MSSP's service when $u_s \geq u_k^{d*}$. Hence, the MSSP's profit will be

$$\pi \leq \left(\bar{a}^2 + \sigma_a^2\right) v^2 \left[\frac{\beta\left(2-\beta\right)}{2c_s} - \frac{1}{2c_k}\right] + d_k \tag{28}$$

The equality holds when $u_s = u_k^{d*}$, which means the MSSP extracts all surplus from clients. And the right hand side of (29) reaches the maximum when $\beta = 1$. However, $u_s = u_k^{d*}$ and $\beta = 1$ are contradicting. In order to have $u_s = u_k^{d*}$, the price p must satisfy the following:

$$p = a_h \beta v - \frac{1}{2}\frac{\left(a_h v\right)^2}{c_k} + \frac{\left(a_h v\right)^2}{c_s}\beta\left(1-\beta\right) \tag{29}$$

$$p = a_l \beta v - \frac{1}{2}\frac{\left(a_l v\right)^2}{c_k} + \frac{\left(a_l v\right)^2}{c_s}\beta\left(1-\beta\right) \tag{30}$$

Since $a_h > a_l$ and $a_h v < c_k$, $\beta = 1$ cannot solve both (30) and (31) together. Therefore, a sufficient small d_k would guarantee that the profit of offering single price is smaller than that of offering two different prices. Hence, the MSSP will offer two prices honestly and it solves the credence good problem.