Association for Information Systems

AIS Electronic Library (AISeL)

CONF-IRM 2018 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2018

Outsourcing Information Security: The Role of Information Leakage in Outsourcing Decisions

Nan Feng
Tianjin University, fengnan@tju.edu

Yufan Chen
Tianjin University, cyf_lana@tju.edu

Haiyang Feng
Tianjin University, hyfeng@tju.edu.cn

Minqiang Li
Tianjin University, mqli@tju.edu.cn

Jie Zhang
The University of Texas at Arlington, jiezhang@uta.edu

OUTSOURCING INFORMATION SECURITY: THE ROLE OF INFORMATION LEAKAGE IN OUTSOURCING DECISIONS

Nan Feng
Tianjin University
fengnan@tju.edu

Yufan Chen
Tianjin University
cyf_lana@tju.edu

Haiyang Feng
Tianjin University
hyfeng@tju.edu.cn

Minqiang Li
Tianjin University
mqli@tju.edu.cn

Jie Zhang
The University of Texas at Arlington
jiezhang@uta.edu

Abstract:
Emerging research regarding the economics of outsourcing information security recommends that firms utilize full outsourcing due to its cost advantages but ignore the risk of information leakage. In our model, we take the information leakage into account, and show that it is necessary for firm to assess the risk before outsourcing. Next, we divide a firm's business operations into core business and non-core business operations and introduce a partial outsourcing strategy. We find that the security quality of partial outsourcing is always lower. Subsequently, we demonstrate the conditions for selecting from among three security strategies, i.e., in-house development, partial outsourcing and full outsourcing. Based on our results, in high-risk information leakage environments, we do not recommend outsourcing. We further demonstrate that outsourcing security of non-core business is an alternative strategy when the risk of information leakage is not high. A firm should shift from outsourcing to developing security protection in-house as the percentage of information assets utilized for core business increases. In addition, our results show that outsourcing information security of only core business is a strictly dominated strategy.

Keywords:
Information security strategy; partial outsourcing; information leakage; managed security service

1. Introduction

The market for managed security services have exploded in popularity over the past few years. According to a report by PwC (2017) almost two-thirds (62%) of their respondents say they use managed security service providers(MSSPs) to operate and enhance their cybersecurity programs. Although information security is crucial, it is no longer necessarily essential for firms to deploy in-house information security protection system. As MSSPs can provide

security expertise at a lower cost with their specialized knowledge and abundant experience, there has been a growing consensus on outsourcing security being a viable option for companies. Measuring the input and output, small firms, which lack both budget and expertise, are tend to choose MSSP's service.

Nevertheless, managed security service(MSS) may not always be the best choice. Firms should consider a particular outsourcing risk, named information leakage. Information leakage happens whenever private information is revealed to unauthorized parties. In the process of information security outsourcing, a third party is given the authority to monitoring the information system through approaches like detecting packets passing through a router, switch or firewall. This means that all communication between a client and server will be send to the monitoring system of MSSP. During this period, the firm usually lose control of their own information. For one thing, the complex network environment may not be that secure as excepted. For another, the MSSP's operation may lead to leakage. Ulltveit-Moe (2014) implies that intrusion detection systems can be configured to leak information due to incorrect operation or intention of malicious insiders. Because it is hard to identify the ascription of liability, the firm, the MSSP or a third party, the loss of information leakage is not covered by MSSP's compensation. IBM (2016) reports that data breaches caused by third party increased the per capita cost from $158 to $172 per record and 25 percent of the data breaches were caused by human factor including contractors. A firm can never neglect the issues of information leakage when outsourcing information security.

Taking account of the risk of information leakage, we further recognize that outsourcing the security of a firm's core business operations may cause a greater loss if information leakage exists. Core business operations (Cho and Chan, 2015) generate major value for the business, activities that are critical to business performance and future benefit, such as enterprise resource planning and product development. We can define the other part as non-core business operations. Consequently, we can decide which security strategy to choose for core business operations and non-core business operations respectively.
Considering both the benefits (e.g. cost advantage) and the risks (e.g. information leakage), there are four strategies available, listed in Table 1.

Table 1. Four Different Strategies

Category of Business Operations	Strategy			
	IN	OF	ONC	OC
Core business	In-house	Outsourcing	In-house	Outsourcing
Non-core business			Outsourcing	In-house

The rest of the paper is arranged as follows. Based on the prior studies regarding information security outsourcing, we demonstrate our analytic model by adding the effect of information leakage to information security outsourcing. This is followed by analyzing the tradeoffs between the different strategies: in-house, partial outsourcing and full outsourcing. Finally, we summarize the conclusion and give suggestions for future research.

2. Literature Review

Our research is built on an economic basis for information security outsourcing. In light of the emergence of MSSPs, Gupta and Zhdanov (2012) demonstrates there are potential benefits to join an MSSP network, including pooling risk, and access to more security-enabling resources and expertise. Zhao et al. (2013) draws a conclusion that MSSPs serve multiple firms might internalize the externalities of security investments and mitigate security investment inefficiencies. Studies regarding outsourcing contract are another primarily subject. Lee et al. (2013) proposes the multilateral contract, which can solve the double moral hazard problem. In regards to the different functions of MSSP services, Cezar et al. (2014) analyzes the necessity of outsourcing prevention and detection to different MSSPs and constructed a penalty-and-reward contract that outsourced both prevention and detection to a single MSSP. Given the multi-client nature of MSSP services, Hui et al. (2012) considers both system interdependency risk and mandatory requirements when firms decided to outsource information security.

A literature review of Hoecht and Trott (2006) shows that outsourcing decision carries the risk of information leakage，which results in the firm' s core competencies being transferred to the wider industry context. From economic aspects, studies that use analytical models to examine information leakage risk in outsourcing are as follows. Anand and Goyal (2009) demonstrates that for both informed and uninformed firms that use common upstream suppliers, information flows intersect through the leakage of demand information to unintended recipients. García-Vega and Huergo (2011) constructs a monopolistic competition model of technology leakage in which outsourcing increased a firm’s fixed transaction. Nimubona and Benchekroun (2015) considers R&D outsourcing in their model and analyzes the effects of involuntary information leakage on firm profits and welfare.

In addition, our study adds to the literature on partial outsourcing. Compared to full outsourcing, partial outsourcing may be understood as a mixture of in-house efforts and fee-for-service outsourcing. Alvarez and Stenbacka (2007) determines that the optimal threshold for establishing partial outsourcing is an increasing function of the underlying proportion of outsourcing. Wang et al. (2007) discovers that in a certain condition, partial outsourcing could also be a viable strategy. Moon (2010) develops a model for partial outsourcing during conditions of market uncertainty to help firms determine an outsourcing strategy and construct a corresponding decision-support system. According to Cho and Chan (2015), considering Software as a Service (SaaS) as a new approach of outsourcing, its cost advantage would induce the adoption for non-core operations whereas its technology advantages would induce the adoption for core business operations.

In contrast to the aforementioned studies, we take account of the disincentive of outsourcing, information leakage, and focus on firms’ decisions about whether to outsource or partial outsource.

3. Model

We consider a firm that seeks to determine whether to outsource its information security or to use an in-house strategy. Prior to this, an information system risk assessment should be implemented to assess the external threats and the value of the information assets. Information assets refer to information resources that support and ensure the firm's business operation, such as information, systems, networks, software, hardware. The assets can be divide by the division of core bossiness and non-core bossiness operation. Based on this division, a firm that decides to outsource information security must make an additional decision regarding a specific outsourcing strategy, i.e., either partial outsourcing or full outsourcing.

For the purpose of describing the security environment of the firm, we model security attacks the firm suffered as follows:

Table 2: Model Notation

Variable	Description
v	Value of information assets that support the firm's all business operations. ($v > 0, v = v_c + v_{nc}$)
v_c	Value of information assets that support the firm's core business operations
v_{nc}	Value of information assets that support the firm's non-core business operations
p	Probability that a hacker will attack the firm's information assets ($0 < p < 1$)
q_m	Level of security quality the MSSP can provide($0 < q_m < 1$)
q_f	The firm's security quality($0 < q_f < 1$)
c_m	Cost coefficient of MSSP
c_f	Cost coefficient of firm
F	Fixed fee paid by the firm to the MSSP
β	Ratio based on compensation from the MSSP to the firm($0 < \beta < 1$)
k	correlation coefficient between F and β
l	The unit loss of information leakage when firm outsource the security of its non-core business ($0 < l < 1$)
d	The ratio of unit loss of core asset's information leakage to that of non-core asset's information leakage.

(dl represents the unit loss of information leakage when firm outsource the security of its core business)

We value the information assets of certain business operations at v, which facing a probability of hacker attack at $p \in (0,1)$. The firm or the MSSP determines the security quality level at q_i. The cost for providing security protection at that level can be expressed as $\frac{1}{2}c_f q_i^2$, according to the alignment in Kai-Lung's model (Hui, 2012). However, there is still possibility of firm's suffering a loss, which we can calculate as $p(1-q_i).(\, i \in \{f,m\})$

When a firm would like to outsource information security to a MSSP, a contract will be sign by the both parties. In this study, we construct a contract that contains two parts. We abstract the first part as a fixed fee F to the MSSP. The second part as $\beta \in [0,1]$ represents the compensation term ('liability'). If the firm suffers a loss of v due to a hacker attack, the MSSP must compensate the firm by βv. Meanwhile, choosing outsourcing strategy means the firm will bear the risk of information leakage. Specifically, the possible losses for outsourcing the security of its non-core business is $v_c dl$ and that of its non-core business is $v_{nc} l$.

Our model encompasses the following assumptions.

Assumption 1: $c_m < c_f$, It ensures that when outsourcing information security to an MSSP, the firm will enjoy a cost advantage, which directly induces it to select outsourcing rather than employing in-house security strategy.

Assumption 2: $0 < q_f < 1, 0 < q_m < 1$, which ensures that the analysis will not arrive at a corner solution.

Assumption 3: $\beta = kF \quad (0 < k < 1)$, which implies the compensation have a linear correlation with the service fee. The more a firm pay, the higher proportion of compensation the MSSP will pay back.

Assumption 4: $d > 1 \; and \; dl < 1$. This assumption implies that outsourcing the security of core business has a larger unit loss based on the information assets' value.

3.1 In-house: Strategy IN

If the firm develops security protection in-house, its expected utility will be

$$u_{in-house} = v(1-p(1-q_f)) - \frac{1}{2}c_f q_f^2 \qquad (1)$$

The first term represents the remaining value after the firm's information assets being successfully attacked. The second term represents the cost of investing in security protection.

3.2 Full Outsourcing: Strategy OF

We model the contracting problem referring to the 1-MSSP-P contract (Cezar, 2014). The sequence of events is as follows.

Stage 1. The firm decides to outsource information security and offers the contract $[F,\beta]$.

Stage 2. If the MSSP accepts the contract, it selects the security quality, q_m, it will provide; otherwise, the game ends.

Stage 3. If the firm is attacked successfully, the MSSP will give a refund calculated by β.

If a firm choose the outsourcing strategy, the expected utility of the firm and the expected payoff for the MSSP are determined as follows:

$$u_{full} = v(1 - p(1 - q_m)) + vp(1 - q_m)\beta - F - v_{nc}l - v_c dl, \quad (2)$$

$$\pi_{full} = F - vp(1 - q_m)\beta - \tfrac{1}{2}c_m q_m^2 . \quad (3)$$

The second term of u_{full}, is the expected compensation the firm would receive. $v_{nc}l + v_c dl$ represents the loss when information assets suffer information leakage. Relatively, for the expression π_{full}, the middle section is compensation the MSSP pays back if it falls preventing the attack. The last term is the cost that the MSSP invests in security protection.

3.3 Partial Outsourcing: Strategy ONC and Strategy OC

Theoretically, there are two specific strategies in partial outsourcing, outsourcing information security of only non-core business and outsourcing information security of only core business. If a firm outsources information security of only non-core business, the expected utility of the firm and the expected payoff for the MSSP are determined as follows:

$$u_{non-core} = v_c\left[1 - p\left(1 - q_f\right)\right] - \frac{1}{2}c_f q_f^2 + v_{nc}[1 - p(1 - q_m)]$$

$$+v_{nc}p(1 - q_m)\beta - F - v_{nc}l, \quad (4)$$

$$\pi_{non-core} = F - v_{nc}p(1 - q_m)\beta - \tfrac{1}{2}c_m q_m^2 . \quad (5)$$

The first term of $u_{non-core}$, represents the utility of the firm from in-house development for core business's security, and the second term is the utility of the firm outsourcing security of non-core business. $v_{nc}l$ represents the loss when information leakage happens to the information assets of non-core business.

Similarly, if the firm outsources only core assets, the firm's utility and the MSSP's payoff are as follows:

$$u_{core} = v_{nc}[1 - p(1 - q_f)] - \frac{1}{2}c_f q_f^2 + v_c[1 - p(1 - q_m)]$$

$$+v_c p(1 - q_m)\beta - F - v_c dl, \tag{6}$$

$$\pi_{core} = F - v_c p(1 - q_m)\beta - \frac{1}{2}c_m q_m^2. \tag{7}$$

4. Solution and Analysis

4.1 In-house

By maximizing the firm's utility in **Section 3.1**, it should select an optimal $q_f^* = (pv)/c_f$.

The best utility for the firm when it chooses in-house development is then

$$u_{in-house}^* = \frac{p^2 v^2}{2c_f} + (1 - p)v. \tag{8}$$

Lemma 1: The security quality of the firm has a positive correlation with the value of information assets and a negative correlation with the cost coefficient of the firm.

4.2 Full Outsourcing

We use backward induction to solve the firm's contracting problem in **Section 3.2**. In Stage 2 of the game, the MSSP determines its optimum quality by maximizing its profit. And we can obtain the MSSP's optimum quality, $q_m^* = \frac{v\beta p}{c_m}$. Anticipating how the MSSP will determine its best response, the firm determines the fixed service fee and the compensation according to their linear relationship, which make up the contract $[F, \beta]$ in Stage 1 of the game.

The solutions are as follows:

$$q_m^* = \frac{1}{2}\left(1 - \frac{1}{kpv} + \frac{pv}{c_m}\right). \tag{9}$$

$$F^* = \frac{kp^2v^2 - c_m + kpvc_m}{2k^2p^2v^2}. \quad (10)$$

$$\beta^* = \frac{1}{2}(1 + \frac{(-1+kpv)c_m}{kp^2v^2}). \quad (11)$$

Lemma 2: The security quality that the MSSP can provide has a positive correlation with the value of information assets and a negative correlation with the MSSP's cost coefficient.

With respect to outsourcing strategy, we summarize the trends of service fee, F^*. When $0 < pv < \frac{2}{k}$, F^* increase rapidly with the increasing of the pv. After that, F^* falls slowly. Thus, in Proposition 1, we demonstrate the characteristic of the contract terms.

Proposition 1: The service fee can firstly increase rapidly and then decrease slowly with the increasing of the estimated loss under no protection. The compensation has the same trend.

pv represents the loss if the firm's assets are unprotected. A firm may estimate the loss of pv for fear that MSSP take little measure to protect its information asset. When the value of assets or the probability of attacks is small, the firm needs to make sure that its assets are not neglected by MSSP. As the estimated loss increases, the firm is willing to pay more money to ensure its assets are under enough protection. Due to the linear correlation, the compensation ratio increases respectively. After the estimated loss more than a certain value, the fixed fee and compensation start to decrease. Owing to the security quality increases as pv increases （based on in Lemma 2）, it is big enough to prevent the firm from being attacked and reduce actual losses. So with the level of security quality increasing, it is less likely to suffer an attack and it is acceptable for the firm to receive a small proportion of compensation.

4.3 Partial Outsourcing

When adapting partial outsourcing strategy, the firm's decision divided into two parts. The firm determines its security quality regarding the value of assets that need to be protect in-house. At the same time, the firm maximizes its expected utility by determining the terms of the contract. We solve the problems respectively as in the previous calculation of in-house strategy and outsourcing stagey. The optimal value of each decision variable is shown in Table 3.

Table 3. Optimal the Value of the Decision Variable

Choice of Strategy	Optimal value		
	q_f	q_m	F
ONC	$\frac{pv_c}{c_f}$	$\frac{1}{2}(1 - \frac{1}{kpv_{nc}} + \frac{pv_{nc}}{c_m})$	$\frac{1}{2k} + \frac{(-1+kpv_{nc})c_m}{2k^2p^2v_{nc}^2}$
OC	$\frac{pv_{nc}}{c_f}$	$\frac{1}{2}(1 - \frac{1}{kpv_c} + \frac{pv_c}{c_m})$	$\frac{1}{2k} + \frac{(-1+kpv_c)c_m}{2k^2p^2v_c^2}$

We describe the in-house part and outsourcing part security quality of Strategy ONC as q_f^c and q_m^{nc}. Similarly, we use q_f^{nc} and q_m^c for those of Strategy OC. Since v_c and v_{nc} are both less than v, and based on Lemma1 and Lemma 2, q_f^c, q_f^{nc} are lower than q_f as well as q_m^c, q_m^{nc} are lower than q_m. The following are several possibilities of the compare of the different security qualities:

(a) If $q_f > q_m$, $q_f > q_m^c$, q_m^{nc}. If the security quality of Strategy IN exceeds the quality of Strategy OF, it will be higher than either security quality of other strategies.

(b) If $q_m > q_f$, $q_m > q_f^c$, q_f^{nc}. If the security quality of Strategy OF exceeds the quality of Strategy IN, it will be higher than either security quality of other strategies.

(c) If $q_f = q_m$, $q_m = q_f > q_m^c$, q_m^{nc}, q_f^c, q_f^{nc}. If the security quality of Strategy IN and Strategy OF are equal, it will be the optimal security level of all strategies.

Overall, we can realize that:

Proposition 2: The security quality of partial outsourcing is always lower than either in-house strategy or full outsourcing strategy.

Partial outsourcing leads to the decrease of security quality to some extent. The security quality is a key issue that should be considered before decision making, especially for firms that have a mandatory security requirement. A risk-averse firm tend to choose in-house or full outsourcing strategy regarding its high standard of security requirement.

The proofs of all the results are in the Appendix.

5. Optimal Decision

We solve previous problems and show the optimal utilities of different strategies in Table 4.

Table 4. Best utility of different strategies

Strategy	Firm's best utility	tab
IN	$\frac{p^2v^2}{2c_f} + (1-p)v$	$u^*_{in-house}$
OF	$(1-\frac{1}{2}p)v + \frac{p^2v^2}{4c_m} + \frac{(kpv-1)^2c_m}{4k^2p^2v^2} - dlv_c - lv_{nc} - \frac{1}{2k}$	u^*_{full}
ONC	$\frac{p^2v_c^2}{2c_f} + (1-p)v_c + \frac{p^2v_{nc}^2}{4c_m} + (1-\frac{1}{2}p)v_{nc} + \frac{(kpv_{nc}-1)^2c_m}{4k^2p^2v_{nc}^2} - lv_{nc} - \frac{1}{2k}$	$u^*_{non-core}$
OC	$\frac{p^2v_{nc}^2}{2c_f} + (1-p)v_{nc} + \frac{p^2v_c^2}{4c_m} + (1-\frac{1}{2}p)v_c + \frac{(kpv_c-1)^2c_m}{4k^2p^2v_c^2} - dlv_c - \frac{1}{2k}$	u^*_{core}

We use proportion α based on value to measure the information assets that support the firm's

core business and the non-core business operations. Specifically, the firm values its core assets at $v_c = \alpha v$, and values its non-core assets at $v_{nc} = (1-\alpha)v$. Subsequently, we compare the utilities of different strategies so as to analyze which are superior and which are inferior.

We view $u^*_{in-house}, u^*_{non-core}, u^*_{core}, and\ u^*_{full}$ as four lines with l and calculate the intersections of these four lines. The results are show in the Table 5.

Table 5. Solutions of four possible strategies

Interactions	Solution
$u^*_{in-house}$, $u^*_{non-core}$	$\frac{1+kpv(-1+\alpha)}{2kv(-1+\alpha)} - \frac{p^2v(1+\alpha)}{2c_f} - \frac{p^2v(-1+\alpha)}{4c_m} - \frac{(1+kpv(-1+\alpha))^2c_m}{4k^2p^2v^3(-1+\alpha)^3})$
$u^*_{in-house}$, u^*_{core}	$\frac{-1+kpv\alpha}{2dkv\alpha} + \frac{p^2v(-2+\alpha)}{2dc_f} + \frac{p^2v\alpha}{4dc_m} + \frac{(-1+kpv\alpha)^2c_m}{4dk^2p^2v^3\alpha^3})$
$u^*_{in-house}$, u^*_{full}	$\frac{-1+kpv}{2kv(1-\alpha+d\alpha)} - \frac{p^2v}{2(1-\alpha+d\alpha)c_f} + \frac{p^2v}{4(1-\alpha+d\alpha)c_m} + \frac{(-1+kpv)^2c_m}{4k^2p^2v^3(1-\alpha+d\alpha)}$
$u^*_{non-core}$, u^*_{full}	$\frac{p}{2d} - \frac{p^2\alpha}{2dc_f} - \frac{p^2v(-2+\alpha)}{4dc_m} + \frac{(-2-2kpv(-1+\alpha)+\alpha)c_m}{4dp^2v^3k^2(-1+\alpha)^2}$
$u^*_{non-core}$, u^*_{full}	$\frac{p}{2} + \frac{p^2v(-1+\alpha)}{2c_f} + \frac{p^2v(1+\alpha)}{4c_m} + \frac{(-1-\alpha+2kpv\alpha)c_m}{4p^2k^2v^3\alpha^2}$

Under the condition of $l_{24} < l < l_{12}$, Strategy ONC is better than both Strategy IN and

Strategy OF. Besides, when Strategy IN is superior to Strategy OF (i.e. $l > l_{14}$), Strategy OC is worse than Strategy IN (i.e. $l > l_{13}$). When Strategy IN is inferior to Strategy OF (i.e. $l < l_{14}$), Strategy OC is also worse than Strategy OF (i.e. $l < l_{34}$). Therefore, we can achieve:

Proposition 3: Strategy ONC is superior when the risk of information leakage is assessed medium. Whereas, Strategy OC is a strictly dominated strategy.

When the risk of information leakage risk is greater, the firm will prefer Strategy IN. This is because the loss caused by the information leakage exceeds the benefit of the MSSP's cost advantage. On the contrary, when the leakage risk is low and the cost advantage is dominant, the firm tends to choose full outsourcing, which would reduce cost and achieve a higher level of security quality. When the risk of information leakage is medium, the firm tends to outsource it is the information security of non-core business. Under this condition, the firm can only bear the loss of non-core information leakage, for the risk of core information is too high.

Next, we discuss the optimal decision by adding another variable to the result above. Fig. 1, Fig. 2, Fig. 3 shows the strategies considering *l* and *p*, *l* and c_m, *l* and α

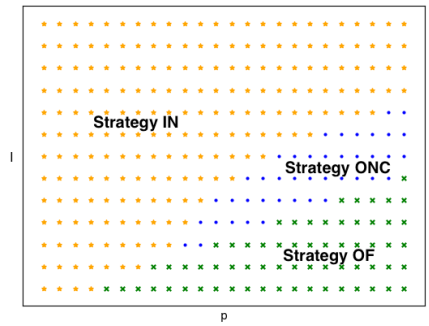

Fig 1. Strategies considering *l* and *p*

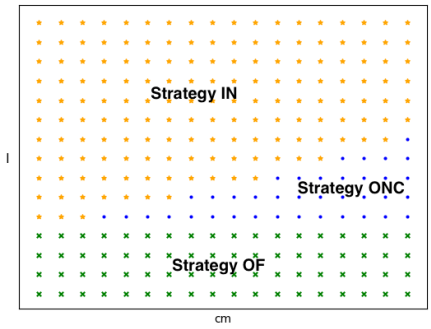

Fig 2. Strategies considering *l*, c_m

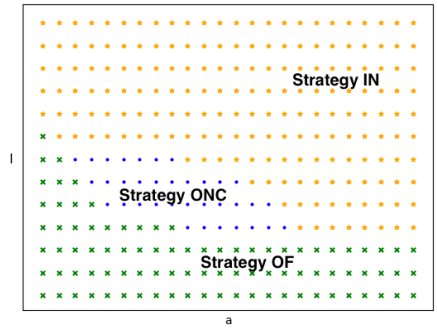

Fig 3. Strategies considering *l* and α

Based on Figures above, all of them are divided into three sections: in-house, partial outsourcing and full outsourcing.

Proposition 4: (a)high information leakage risk induce in-house strategy.

(b) low information leakage risk induces full outsourcing strategy

(c) medium information leakage risk may lead to partial outsourcing strategy (Strategy ONC), especially when the firm facing high probability of hacker attack and unobvious cost advantages.

Based on Fig. 1, we considered the risk of both hacker attack and information leakage. Full outsourcing is optimal when the firm under high attack risk and low information leakage risk. Along with the information leakage risk going up, the firm will take measures to prevent its information from being leaked. During this process, the optimal strategy will change firstly to Strategy ONC and finally to Strategy OF. Fig. 2 implies, under the condition of medium information leakage risk and an obvious cost advantage, the firm tend to outsource information security of all its business operations. Based on Fig. 3, we estimate whether the percentage of core assets is high or low. The optimal decision is Strategy OF when the information leakage risk is low. When the percentage of core assets is in a certain range, as well as the likelihood of information leakage risk is medium, the optimal decision is Strategy ONC. However, the optimal decision is Strategy IN when both the percentage of core assets and the information leakage risk are high.

6. Conclusions

Numerous studies regarding information security outsourcing assume that when firms make a decision to outsource, they gain more benefits than they would by utilizing in-house development and that cost advantages are the only consideration of firms when making this decision. However, outsourcing may not always achieve more utility for firms than in-house development. In contrast to prior studies, we consider the information leakage and introduce a partial outsourcing strategy. Partial outsourcing strategy cannot reach the optimal security quality among the four strategies, but sometimes it is effective to reduce the risk of information leakage. Based on our results, we determine that full outsourcing is not the optimal solution when the risk of information leakage is great and using a partial outsourcing strategy can mitigate the risk partly. For non-core business, outsourcing security has a low potential leakage loss. Hence, outsourcing information security of non-core business is an alternative strategy when this part of assets occupies a larger percentage. However, outsourcing information security of core business is a strictly dominated strategy because it is generally either worse than full outsourcing when risk of information leakage seems low or worse than in-house development when risk of information leakage is high. As the percentage of core assets increases, the firm's security strategy will shift from outsourcing to in-house development. Thus, information leakage risk is an essential issue for firms' decision makers to consider.

This research may be extended in several directions. One possibility is to analyze the effect of the parties' risk aversion on the optimum contract terms. Another possibility is to analyze how the optimal strategy would change considering interdependent risk between non-core business and core business operations.

Appendix

Proof of Lemma 1:

For in-house strategy, the first-order conditions for optimality utility is

$$\frac{\partial u_{in-house}}{\partial q_f} = pv - c_f q_f = 0. \qquad \text{(A.1)}$$

We can get

$$q_f^* = \frac{pv}{c_f}. \quad \text{(A.2)}$$

It's obvious that q_f^* has a positive correlation with v and a negative correlation with c_f.

Proof of Lemma 2:

For outsourcing strategy, firstly, in order to maximizing π, we calculate the following equation:

$$\frac{\partial \pi}{\partial q_m} = pv\beta - c_m q_m = 0. \quad \text{(A.3)}$$

We can get the MSSP's optimum quality:

$$q_m^* = \frac{v\beta p}{c_m}. \quad \text{(A.4)}$$

Then we determine the contract term $[F, \beta]$. Through Assumption 3, we can transform $u_{outsourcing}$ into a function of F. This way, we can get the optimal payment by calculating:

$$\frac{\partial u_{full}}{\partial F} = -1 + kpv + \frac{k(1-2Fk)p^2v^2}{c_m} = 0. \quad \text{(A.5)}$$

We can get the optimum fee:

$$F^* = \frac{kp^2v^2 - c_m + kpvc_m}{2k^2p^2v^2}. \quad \text{(A.6)}$$

According to Assumption 3, We can get the optimum compensation:

$$\beta^* = \frac{1}{2}\left(1 + \frac{(-1+kpv)c_m}{kp^2v^2}\right). \quad \text{(A.7)}$$

Substituting F^* in q_m^* and u_{full}^*, we can obtain the MSSP's optimum quality:

$$q_m^* = \frac{1}{2}\left(1 - \frac{1}{kpv} + \frac{pv}{c_m}\right), \quad \text{(A.8)}$$

and the best firm's utility when outsource its information security is:

$$u_{full}^* = \frac{1}{4}\left(-\frac{2}{k} + 4v - 2pv + \frac{p^2v^2}{c_m} + \frac{(-1+kpv)^2c_m}{k^2p^2v^2} - 4dlv_c - 4lv_{nc}\right). \quad \text{(A.9)}$$

In order to characterize q_m^*, the first-order derivative calculation shows below:

$$\frac{\partial q_m}{\partial v} = \frac{1}{2}\left(\frac{1}{kpv^2} + \frac{p}{c_m}\right) > 0. \tag{A.10}$$

$$\frac{\partial q_m}{\partial c_m} = -\frac{pv}{2c_m^2} < 0. \tag{A.11}$$

The results above lead to the same conclusion as that of q_f^*

Proof of Proposition 1:

In order to characterizes F^*, calculate the first-order derivative of F^* with pv:

$$\frac{\partial F^*}{\partial pv} = \frac{(2-kpv)c_m}{2k^2p^3v^3}, \tag{A.12}$$

And the solution is:

When $0 < pv < \frac{2}{k}$, F^* firstly increase rapidly then decrease slowly with the increasing of the pv. According to Assumption 3, β^* has the same trend as F^*.

we illustrate the above analysis with numerical examples. As is show in Fig 4.

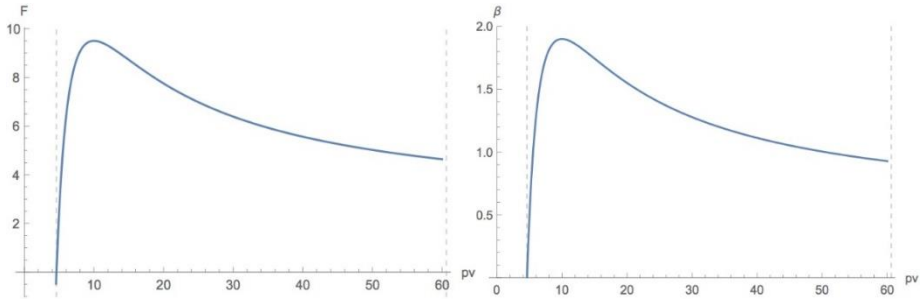

Fig 4. Variation F and β^* trend with $k = 0.2,\ c_m = 56$

Proof of Proposition 3:

$$l_{14} - l_{13} = \left[\frac{-1+kpv}{2kv(1-\alpha+d\alpha)} - \frac{-1+kpv\alpha}{2dkv\alpha}\right] + \left[-\frac{p^2v}{2(1-\alpha+d\alpha)c_f} - \frac{p^2v(-2+\alpha)}{2dc_f}\right]$$

$$+ \left[\frac{p^2v}{4(1-\alpha+d\alpha)c_m} - \frac{p^2v\alpha}{4dc_m}\right] + \left[\frac{(-1+kpv)^2c_m}{4k^2p^2v^3(1-\alpha+d\alpha)} - \frac{(-1+kpv\alpha)^2c_m}{4dk^2p^2v^3\alpha^3}\right]$$

$$= -\frac{(-1+\alpha)(1+(-1+d)kpv\alpha)}{2dkv\alpha(1+(-1+d)\alpha)} - \frac{p^2v(2+d(-1+\alpha)-\alpha)(-1+\alpha)}{2d(1+(-1+d)\alpha)c_f}$$

$$-\frac{p^2v(-1+\alpha)(d-\alpha+d\alpha)}{4d(1+(-1+d)\alpha)c_m}+\frac{(-1+\alpha)(d\alpha(1+\alpha-2kpv\alpha)+(-1+kpv\alpha)^2)c_m}{4k^2p^2v^3\alpha^3(d+(-1+d)d\alpha)}$$

We can get $l_{14}-l_{13}>0$, which means if $l>l_{14}$, then $l>l_{13}$.

So when Strategy IN is superior to Strategy OF (i.e. $l>l_{14}$), Strategy OC is worse than Strategy IN (i.e. $l>l_{13}$).

In the same way, we can get $l_{34}-l_{14}>0$, then $l_{34}>l_{14}$. In other words, When Strategy IN is inferior to Strategy OF (i.e. $l<l_{14}$), Strategy OC is also worse than Strategy OF (i.e. $l<l_{34}$). Therefore, we can achieve:

References

Alvarez, L. H. R., & Stenbacka, R. (2007). Partial outsourcing: A real options perspective. *International Journal of Industrial Organization, 25*(1), 91-102.

Anand, K. S., & Goyal, M. (2009). Strategic Information Management under Leakage in a Supply Chain. *Management Science, 55*(3), 438-452.

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2014). Outsourcing Information Security: Contracting Issues and Security Implications. *Management Science, 60*(3), 638-657.

Cho, V., & Chan, A. (2015). An integrative framework of comparing SaaS adoption for core and non-core business operations: An empirical study on Hong Kong industries. *Information Systems Frontiers, 17*(3), 1-16.

García-Vega, M., & Huergo, E. (2011). Determinants of International R&D Outsourcing: The Role of Trade. *Review of Development Economics, 15*(1), 93–107.

Gupta, A., & Zhdanov, D. (2012). Growth and sustainability of managed security services networks: an economic perspective. *Mis Quarterly, 36*(4), 1109-1130.

Hoecht, A., & Trott, P. (2006). Outsourcing, information leakage and the risk of losing technology-based competencies. *European Business Review, 18*(5), 395-412.

Hui, K.-L., Hui, W., & Yue, W. T. (2012). Information Security Outsourcing with System Interdependency and Mandatory Security Requirement. *Journal of Management Information Systems, 29*(3), 117-156.

Lee, C. H., Geng, X., & Raghunathan, S. (2013). Contracting Information Security in the Presence of Double Moral Hazard. *Information Systems Research, 24*(2), 295-311.

Moon, Y. (2010). Efforts and efficiency in partial outsourcing and investment timing strategy under market uncertainty. *Computers & Industrial Engineering, 59*(1), 24-33.

Nimubona, A. D., & Benchekroun, H. (2015). Environmental R&D in the Presence of an Eco-Industry. *Environmental Modeling & Assessment, 20*(5), 491-507.

Ulltveit-Moe, N. (2014). A roadmap towards improving managed security services from a privacy perspective. *Ethics & Information Technology, 16*(3), 227-240.

Wang, L. M., Liu, L. W., & Wang, Y. J. (2007). Capacity decisions and supply price games

under flexibility of backward integration. *International Journal of Production Economics, 110*(1–2), 85-96.

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements. *Journal of Management Information Systems, 30*(1), 123-152.