

To Share or Not to Share:

Supplier Choice and Customer Demand Reactions to Adverse Events

1. Introduction

Firms look to obtain capabilities through outsourcing relationships. For example, IT cloud service providers are one avenue where benefits such as better security, lower transaction costs, scalability, and agile response to rapid changes in demand can be obtained. However, these benefits do not come without risks. In 2012, lightning in Washington caused Amazon cloud-service outages, bringing down servers for Netflix, Instagram, Pinterest and others (Kosner, 2012). Hackers breached the Amazon cloud in their attack against the Sony Playstation Network, resulting in one of the largest online data breaches in history (Bloomberg News, 2011).

Still, partnerships can provide much needed flexibility. High-tech or other highly dynamic industries may want to obtain capabilities through partnerships rather than in-house development (Barney, 1999), even though sharing a supplier may expose firms and their competitor to same risk, negatively affecting an entire industry (Cleeren et al., 2008; Dyer & Singh, 1998; Parmigiani et al., 2011; Wu et al., 2015). For example, 2011 saw significant events such as the Epsilon breach which exposed customer names and email addresses for a wide range of client organizations, including Chase, Kroger, and Best Buy (Bradley, 2011; Horowitz, 2011; Schwartz, 2011) as well as the breach of the Korean software company, ESTsoft, where update servers infected with malware resulted in exposure of personal information for 35 million South Koreans (Hee-jin, 2011; Hyung-eun, 2011; The Register, 2011). These data breaches have

parallels in the physical product environment. It has been shown that when two brands share a supplier, the stronger brand will recover more quickly after a product recall although, at least for some period of time, customers lose faith in all products in this category (regardless of brand), resulting in reduced sales for all brands (Cleeren et al, 2008).

For situations where incidents and attacks may be directed at a firm's supplier, the firm's customers may be adversely affected. Firms can invest in suppliers in order to improve the security and safety of their supply chain. Firm spending on the supplier could be viewed as either an investment in the supplier (i.e., an extension of the firm boundary) or it could be viewed as the fee paid to execute a particular service level agreement (SLA). In the case of a managed security service provider (MSSP), the supplier learns from providing service to one firm and this naturally provides benefits to other firms using this supplier (Cezar et al., 2010).

In many cases, firms can strategically choose their suppliers, but these suppliers may quite likely have differing adverse event arrival rates. This paper examines supplier choice under different direct- and cross-risk elasticity of customer demand reactions to adverse events. Using game theory and Markov chains to model the problem, we examine the equilibrium firm investment in supplier to reduce adverse event realization, as well as equilibrium firm profits. We compare the case when firms share a supplier to the case where the firms work with independent suppliers. We find that in highly competitive settings (i.e., high negative cross-risk elasticity of demand to adverse events), firms benefit from sharing suppliers even when relative risk of the shared supplier is substantially higher than the independent supplier. We show that as the relative risk of the shared supplier decreases, the shared supplier option is increasingly adopted by firms facing less negative, and eventually positive, cross-risk elasticity of demand.

The paper is organized as follows. In Section 2, we present prior research in this area. Section 3, explains basics of the duopoly model, and then presents both cases of firms investing in independent suppliers and a firms investing in a shared supplier. Section 4 provides the comparison between the shared and independent supplier strategies. Section 5 illustrates how the results change with different attack arrival rate ratios for the independent versus the shared suppliers cases. Section 6 examines the impact of regulation and cooperation, and Section 7 concludes the paper.

2. Literature Review

Information sharing in the supply chain is a popular topic; however, the focus is generally on sharing between partners to improve supply chain efficiency (e.g. Cachon & Fisher, 2000; Ha & Tong, 2008; Kelle & Akbulut, 2005; Ojala & Hallikas, 2006; Tsung, 2000; Zhou & Benton, 2007). Information sharing between competitors has also received attention (Gal-Or & Ghose 2005, Gnyawali & Madhavan 2001). Liu, et al. (2011) discuss information sharing and investment activities in the context where, for example, information at different firms could be complementary or substitutable. The entire industry may accrue benefits when when more sophisticated partners aid the less sophisticated partners with the adoption of information technology, both when suppliers assist their customers (Cheng & Nault, 2012; Wagner & Bode, 2014) and when firms invest in supplier capabilities (Wang & Seidmann, 1995) where the positive spillover along a value chain is based on process-level integration (Tallon, 2011).

Sharing of information security information has been recognized as beneficial (Gordon et al., 2003; Hausken, 2006), with coordination mechanisms, such as Information Sharing and

Analysis Centers (ISACs) (Gal-Or & Ghose, 2005) or customer demand changes (Kolfal et al., 2013) playing a role in facilitating this sharing. August, et al. (2014) examine the impact of information security needs on pricing decisions of cloud service providers.

Kolfal et al. (2013) use customer demand changes as the driver for security investments. In the Kolfal et al. (2013) paper, the security investment could be coordinated between firms, but could only be invested in the firm's own security. We extend Kolfal et al. (2013) model to incorporate both supplier choices of independent and shared supplier and to compare the two models. This enables us to find the optimal firm strategy when faced with these two choices.

3. The Model

We consider a game-theoretic approach with two symmetric profit maximizing firms (duopoly) where firms have two strategic choices for their suppliers. They can either invest in independent suppliers, or share a single supplier. The investments increase security and safety of suppliers, and decrease the arrival rate of realized adverse events at the supplier. The adverse events or incidents at suppliers can probabilistically carry over to firms and affect them as well. Thus, fewer adverse events at the supplier level results in fewer adverse events at the firms that work with that supplier. Firms that are affected by an incident at the supplier, suffer loss of demand for the duration when the incident is realized. The firms are also affected by incidents that occur at the other firm through customer demand reactions, as presented in Kolfal et al. (2013). These demand relations are further explained later in this section. Here we explain the different aspects of the model, however, for brevity, the details of the calculations are not provided in this paper, and are available upon request. The model variables and parameters are provided in Table 1.

Table 1. Model Parameters and Variables

Notation	Definition
c_i	Firm i 's spending in its supplier, $c_i \geq 0$
Λ	Total adverse event or incident arrival rate to the industry, $\Lambda \geq 0$
Λ_k	Adverse event arrival rate to supplier k , $0 \leq \Lambda_k \leq \Lambda$
λ_k	Effective or realized adverse event arrival rate to supplier k , $\lambda_k \leq \Lambda_k$
I_k	Set of firms who invest (and work with) supplier k
$1/\mu$	Expected duration of time that a realized adverse event affects a supplier
$S^s(t)$	Set of possible supplier states
$S(t)$	Set of possible firm states
P_c^i	Cascade probability for an incident at supplier to carry over to the firm i that works with that supplier.
$P_{S(t)}$	Firm steady-state probabilities for firms state $S(t)$,
$D_{i,S(t)}$	Firm i 's demand for firms state $S(t)$
Z_1	Firm direct-risk elasticity of demand, $0 \leq Z_1 \leq 1$
Z_2	Firm cross-risk elasticity of demand, $-1 \leq Z_2 \leq 1$
Π_i	Firm i 's long-run average profit
π	Firm per unit profit excluding the spendings in supplier, $\pi \geq c_i$
v	Relative incident arrival rate of the shared supplier versus the independent supplier, $v \geq 1$

Investment in Suppliers and Adverse Event Arrival Rate: We assume each firm invests in at most one supplier. We denote firm i 's spending in its supplier by c_i where $i = 1, 2$. In the base model,

we assume that the total arrival rate of adverse events in an industry, whether there is one supplier or two, is fixed and follows a Poisson process with rate Λ . One justification for having a fixed total arrival rate can be due to limited resources available to the organizations that cause the incidents, for example limited number of hackers in the IT security context. This assumption will be relaxed in Section 5, where we explore other possibilities.

The arrival rate is divided between the suppliers in the industry; if there are two suppliers in an industry, the arrival rate to each supplier k will be $\Lambda_k = \Lambda/2$. However, not all adverse events are effective; only those incidents that are not prevented and become public knowledge are deemed effective. The effective or realized incident arrival rate that is experienced by each supplier k is denoted by λ_k . Firms can reduce the rate of adverse events at the supplier level by investing in the supplier they are working with. We assume that the effective incident arrival rate is inversely related to the total spendings in the supplier, that is $\lambda_k = \Lambda_k / (\sum_{i \in I_k} c_i)$ where I_k denotes set of all firms who invest in supplier k . When an adverse incident is realized at a supplier, its effects last for a random duration of time according to an exponential function with expected length of $1/\mu$. If the adverse event at the supplier carries over to the firm that works with this supplier, the demand for the firm will be affected during the duration. We will describe how the adverse events on suppliers are carried over to firms later in this section.

Supplier State Probabilities: The suppliers' state process is represented by either

$$S^s(t) = \{S_1^s(t)\} \text{ or } S^s(t) = \{S_1^s(t), S_2^s(t)\} \text{ depending on the number of suppliers in the}$$

industry, with $S_k^s(t)$ denoting the state of supplier k at time t . Considering the effect of adverse events, at any point in time each supplier is either in a “good” or “bad” state, denoted by $S_k^s(t) = G$ or $S_k^s(t) = B$, respectively. The possible states are simplified as $S^s(t) = \{G, B\}$ in the case with one supplier, and $S^s(t) = \{GG, GB, BG, BB\}$ in the case with 2 suppliers.

Firm State Probabilities: We assume that an effective incident at a supplier will carry over to the firm or firms which are using the service from this supplier, with a fixed probability. More specifically, we assume that if an incident is realized at the supplier level, there is a cascade probability P_c^i that the firm i which is working with this supplier is also affected, and this probability is independent from the cascade probability of the other firm. We further assume symmetry, where $P_c^1 = P_c^2 = P_c$. We are interested in cases where $P_c > 0$. Similarly to the supplier states, we denote the state of firms as $S(t) = \{gg, gb, bg, bb\}$ and their probabilities as P_{gg}, P_{gb}, P_{bg} , and P_{bb} .

Demand: The effective adverse events that are carried over to firms will affect the demand for both firms. An adverse event at each firm has a negative effect on its demand, and can have negative or positive effect on the other firm's demand. The normalized demand for firm i when the firms are in state S is denoted by $D_{i,S}$ and is calculated as:

$$\begin{aligned}
 D_{i,gg} &= 1, \text{ for } i = 1, 2 & D_{i,bb} &= 1 - Z_1 - Z_2, \text{ for } i = 1, 2 \\
 D_{1,gb} &= D_{2,bg} = 1 - Z_2 & D_{1,bg} &= D_{2,gb} = 1 - Z_1
 \end{aligned} \tag{1}$$

where Z_1 is the percentage change in demand due to an adverse event in one's own firm, or the direct-risk elasticity of demand and Z_2 is the percentage change in demand due to an adverse event in the other firm, or the cross-risk elasticity of demand. The demand cannot be negative and an adverse event affecting a firm cannot increase its demand, thus $Z_1 \in [0, 1]$. We assume that when an adverse event affects one firm, the other firm cannot gain or lose more than the other firm's demand loss or gain, that is $Z_2 \in [-1, 1]$. Moreover, we only consider the cases with $Z_1 + Z_2 \leq 1$ and $Z_1 + Z_2 \geq 0$ which ensure that $D_{i,bb} \geq 0$ and $D_{i,bb} \leq 1$ hold. Finally, we consider the cases where the impact of events at one firm is greater than the impact of events at the other firm, thus $Z_1 \geq |Z_2|$. According to Kolfal et al. (2013), we use the terms substitutes in loss, unaffected by loss, and complements in loss for the cases of $Z_2 < 0$, $Z_2 = 0$, and $Z_2 > 0$, respectively.

Profit: Each firm in this model maximizes its long-run average profit. It is assumed that the per unit profit excluding investment in suppliers, π , is known and fixed. The long-run average profit

for firm i is given as $E[\Pi_i] = \lim_{T \rightarrow \infty} E[\frac{1}{T} \int_0^T D_i(t)(\pi - c_i)Q dt]$. We require $\pi - c_i > 0$, as a

participation constraint, as otherwise the firm would not be willing to continue operation. By using the demand equations we can write this equation in its steady-state form as

$$E[\Pi_i] = (P_{gg} D_{i,gg} + P_{bg} D_{i,bg} + P_{gb} D_{i,gb} + P_{bb} D_{i,bb})(\pi - c_i)Q \quad (2)$$

3.1 Investment in Independent Suppliers

In this case, each firm works with its own independent supplier, and the suppliers of the two firms are independent of each other. The model setting can be explained as in Figure 1. Each of the two suppliers get half of the total incident arrival rate to the system. When an incident occurs at supplier, it may carry over to the firms that work with that supplier with a certain probability. The model can be used to calculate the equilibrium spending and equilibrium expected profit. For brevity, the calculations are not provided here, and are available upon request.

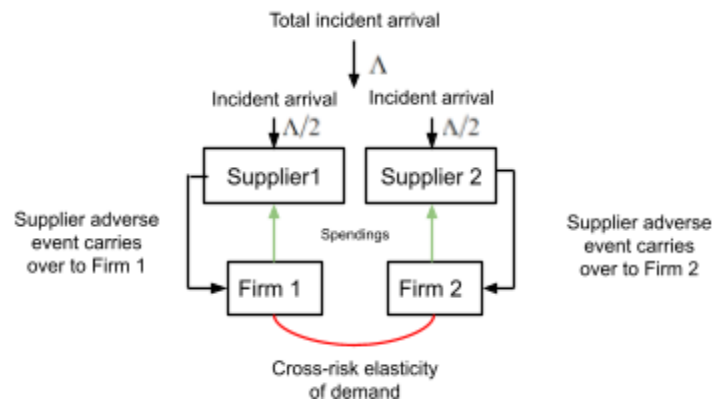


Figure 1. Model Setting for Two Firms with Independent Suppliers

3.2. Investment in Shared Supplier

The next strategic option for the firms is for them to spend equally on a shared supplier. The model setting for this case is provided in Figure 2 below. Since there is only one supplier present in this case, the incident arrival rate at the supplier is equivalent to the total incident rate for the industry, thus $\Lambda_k = \Lambda$. Then we use the model settings to calculate the equilibrium spending and equilibrium expected profit. Again, for brevity, the calculations are not provided here, and are available upon request.

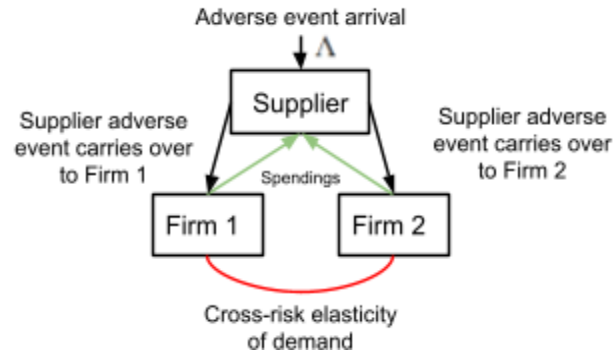


Figure 2. Model Setting for Two Firms with Shared Supplier

4. Comparing Shared Supplier Design versus Independent Supplier Design

In this section, we compare these two strategic options to find out the conditions at which each option yields higher profit for the firms by examining the equilibrium expected profits in sections 3.1 and 3.2. Because the two models differ only in the supplier structure, we can directly compare them. Lemma 1 provides the conditions for each of these decisions to be optimal. The proof is available upon request.

Lemma 1. Comparing independent suppliers versus shared supplier strategies we have:

- (i) When $Z_2 > 0$, equilibrium expected profit in the independent suppliers case is higher than the shared supplier case.
- (ii) When $Z_2 < 0$ and $Z_1 > -2Z_2$, equilibrium expected profit in independent suppliers case is higher than the shared case.
- (iii) When $Z_2 < 0$ and $Z_1 < -2Z_2$, equilibrium expected profit in shared supplier case is higher than the independent supplier case.

(iv) Equilibrium expected profits are the same for the independent and shared supplier cases when $Z_2 \leq 0$ and $Z_1 = -2Z_2$. ◊

The regions in which each of the two options are optimal in the feasible region is provided in Figure 3 below.

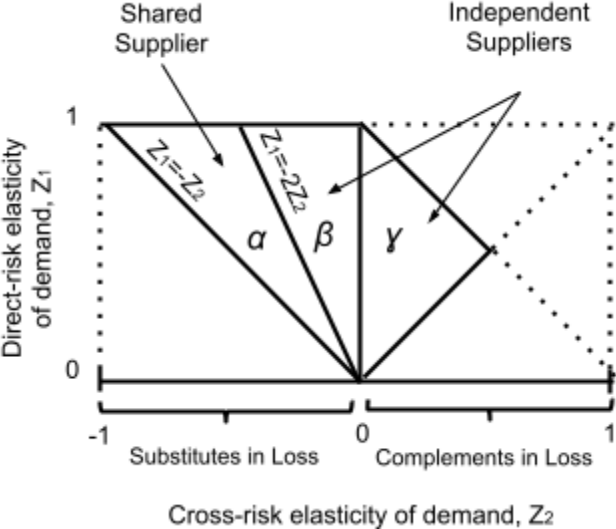


Figure 3. Comparing Independent Supplier versus Shared Supplier Strategies

The regions α (shared supplier, substitutes in loss customer demand reaction), β (independent supplier, substitutes in loss customer demand reaction), and γ (independent supplier, complements in loss customer demand reaction) correspond to points 1, 2 and 3 in Lemma 1, respectively. When firms are substitutes in loss (i.e. $Z_2 < 0$), then there is a threshold value of cross-risk elasticity, $Z_1 = -2Z_2$, below which the optimal choice is for firms to share the supplier (region α). Above the threshold (region β), the firms should choose independent suppliers. When firms are complements in loss (i.e. $Z_2 > 0$, region γ), they should also choose independent suppliers. What this implies is that firms are more inclined to utilize shared

suppliers when there is more competition between the firms (firms are substitutes in loss).

However, if there is competition between firms, the decision to share or not to share suppliers also depends on the direct-risk elasticity of demand.

5. Effect of Attack Arrival Rates on The Model

In the case of independent suppliers described in Section 3.1, we assumed the incident arrival rates for the two suppliers to be $\Lambda_k = \Lambda/2$. This can be true under the assumption that total incident arrival rate in an industry remains the same. However, in other settings, this may not be the case. Here, we investigate the effect of different attack arrival rates on the strategic decision of choosing between independent suppliers versus shared supplier. We consider this by changing the attack arrival rate for each of the two suppliers to be $\Lambda_k = \Lambda/v$, where $v > 1$. v represents the relative incident arrival rate of the shared supplier case to independent suppliers. In the baseline model described in Section 3, we have $v = 2$. For $v > 2$, the arrival rate for the independent is lower than the baseline model, and for $v < 2$, it is higher than the baseline model. Figure 4 illustrates how the optimal regions change when the ratio of arrival rates for the independent over shared supplier case change.

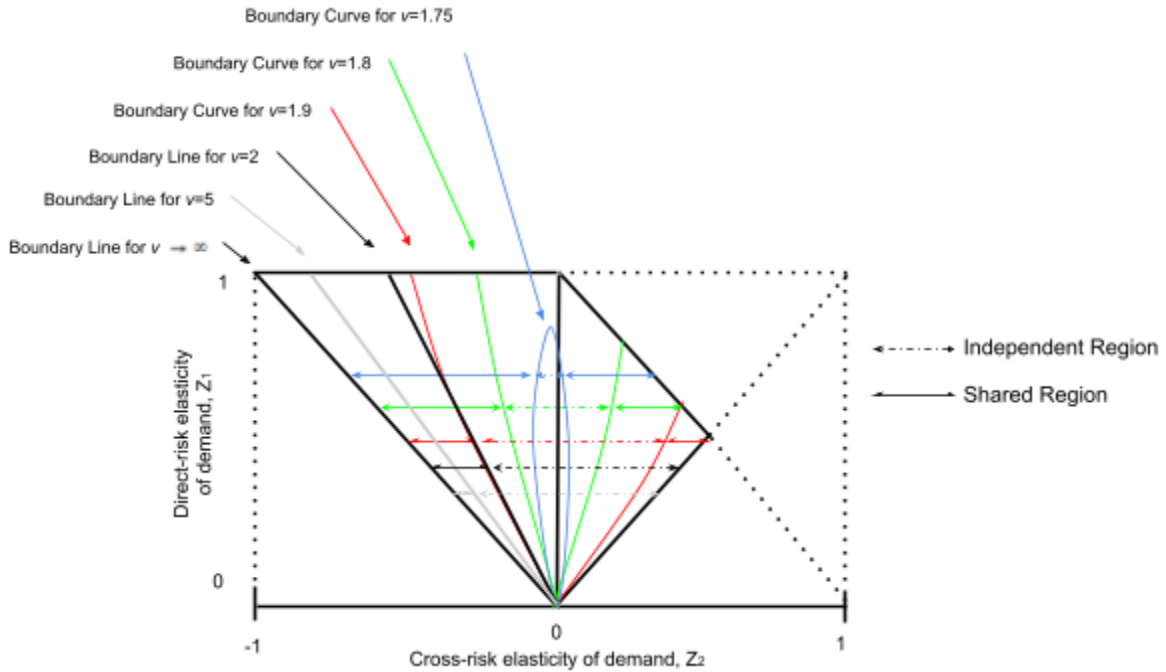


Figure 4. Independent versus Shared Strategies with Various Incident Arrival Rate Ratios

It can be seen that as v increases, or as the relative attack arrival rate of the independent suppliers decreases, the region in which the shared supplier case is optimal becomes smaller and smaller. This is intuitive, as increase in v means that the attack arrival rate in the independent case decreases as compared to the shared case, and so the independent suppliers become more desirable for the firms. When the attack arrival rate for the independent supplier case approaches Λ/∞ , the boundary line between the regions approaches the line $Z_1 = -Z_2$ (the 45 degree line).

On the other hand, a very interesting phenomenon can be seen for $1 < v < 2$. In this region, there are two boundary curves between the shared versus independent suppliers. As v decreases, or the relative attack arrival rate of the independent suppliers increases, the region for independent suppliers shrinks. In Figure 4, for $v < 2$ we can see that independent suppliers are

optimal in the middle region, and shared supplier is optimal in the two regions on the sides. We can see for $\nu = 1.8$ that as the relative arrival rates become more even, the independent region shrinks on both sides and for $\nu = 1.75$ the region for independent suppliers shrinks to an asymmetric ellipsoid, skewed toward negative values of cross-risk elasticity of demand, Z_2 .

6. Effect of Regulation and Cooperation

In this section, we examine the effect of regulation and industry cooperation using the models described in Section 3. In some industries, a minimum required spending, or regulated spending R can be set on the firms' security investment. This can be seen either as regulation, or as cooperation among firms in order to improve their profit. Here, we refer to both of these actions simply as regulation. If the required security spending is less than the equilibrium spending, then this regulation has no effect on the firms' spending. However, if it is higher than the equilibrium spending, then it will cause firms to increase their spending levels to R . Based on the model parameters, the regulation can increase or decrease firm profits. Here we assume that the regulation is set to the point that it maximizes firm profit, and call this the optimal regulation. In Figure 5, we analyze this in a special case. For the case of independent suppliers we find that firm profit can increase under regulation only in the complements in loss case, much as discussed in Kolfal et al. (2013).

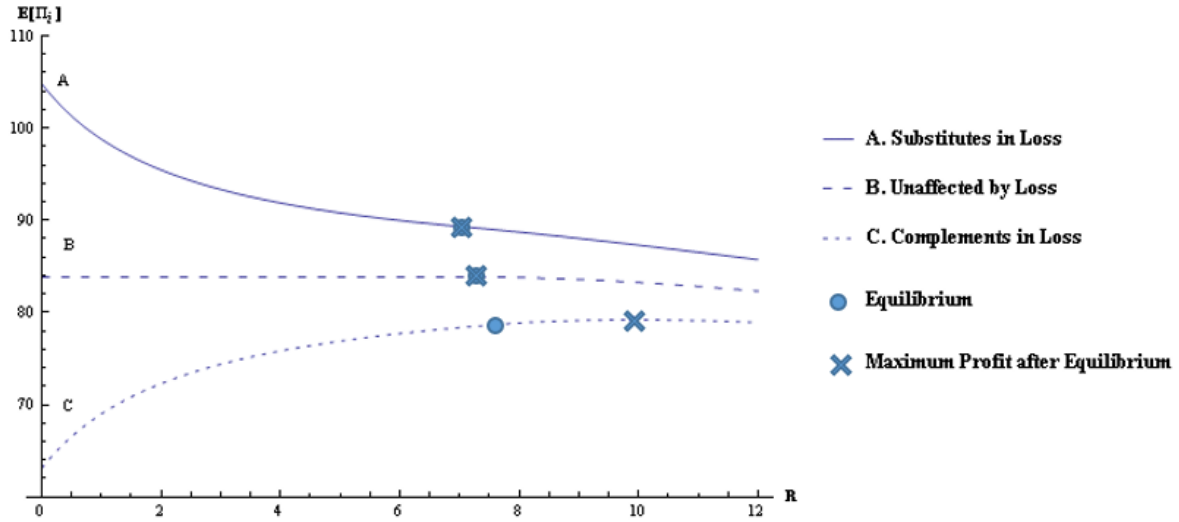


Figure 5. Expected Profit for Required Investment Spending in Independent Case

In the case of shared supplier, we find that regulated spending can increase profit over all values of cross-risk elasticity, as illustrated in Figure 6.

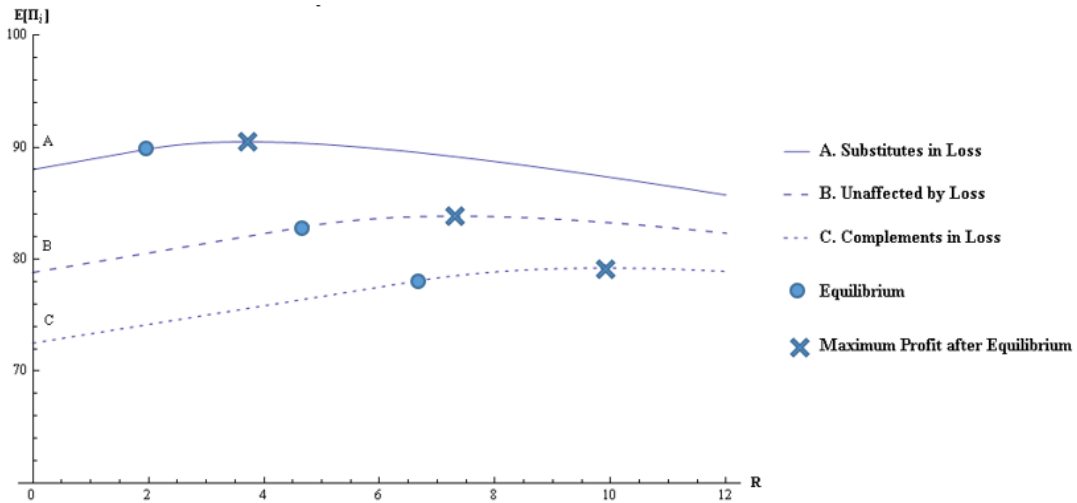


Figure 6. Expected Profit for Required Investment Spending in Shared Case

In order to better understand the difference between the two strategic options, we analyze the two options of independent and shared suppliers for each market environment of regions α , β , and γ as explained in Figure 3. We determine both the optimal strategic decision and whether or not regulation will improve or diminish the profit making of the firms. The complete analysis is available upon request. Table 2 summarizes these results. We can see that the best strategy of either going with shared or independent suppliers, depends on the particular combination of direct- and cross-risk elasticity of demand that a firm faces, and also whether or not optimal regulation is imposed.

Table 2. Summary of Comparison Between Independent versus Shared Strategies

Case	Region	Expected Profit at Equilibrium (Without Regulation)	Does Optimal Regulation Increase Expected Profit?	Expected Profit under Optimal Regulation
i	α	Shared > Independent	Yes	Shared > Independent
ii	Boundary between α and β	Shared = Independent	Yes	Shared > Independent
iii	β	Shared < Independent	Yes	Shared > Independent
iv	Boundary between β and γ	Shared < Independent	No	Shared = Independent
v	γ	Shared < Independent	Yes	Shared = Independent

It can be seen that when optimal regulation is imposed, the shared strategy is never dominated by the independent strategy. This implies that when optimal regulation exists, firms are willing to share suppliers, because the optimal regulation adds a layer of guarantee to the shared supplier choice, and prohibits free-rider possibility. This can also be seen in reality, as coalitions are more common in the highly regulated markets.

7. Conclusions

A key finding of our work is the identification of specific combinations of direct- and cross-risk demand reactions to adverse IT security events, where it is best to share resources and

synchronize risks through a shared supplier. This paper contributes to the literature by providing a framework for comparing the two strategic choices, which was not previously analyzed in the literature. For example, while Kolfal et al. (2013) consider the problem of when to strategically cooperate, we go one step further. We show how the decision-making of the firms when they have the choice of either independent or shared supplier, affects the dynamics of the game, and the structure of the supply chain. We find that in highly competitive markets, firms benefit from sharing suppliers even when relative risk of the shared supplier is relatively higher than the independent supplier. On the other hand, when relative risk of the shared supplier decreases, the shared supplier option becomes increasingly desirable for firms. In order to make the optimal decision, the relative differences in adverse event arrivals between supplier alternatives must be considered in conjunction with the direct- and cross-risk elasticities of demand.

Our results with respect to IT supply chain design support the analysis of Gal-Or and Ghose (2005) who find that cooperation and information sharing in security problems between firms is greater in competitive markets. However, it seems that Gal-Or and Ghose (2005) discuss only half the story. We also show that when the relative adverse event arrival rates to the shared supplier decrease, even when firms are complements in loss (the other extreme of competition), they are motivated to share suppliers. Moreover, we show that regulation and cooperation can be beneficial to the firm profits in many cases, and generally, regulation can enhance profits in the shared supplier case.

References

August, T., Niculescu, M.F., & Shin, H. (2014) **Cloud Implications on Software Network Structure and Security Risks**. *Information Systems Research*. 25(3):489-510.

Barney, J.B. (1999) **How a firm's capabilities affect boundary decisions**. *Sloan Management Review*. 40(3): 137-145

Bloomberg News (2011). **Sony Network Breach Shows Amazon Cloud's Appeal for Hackers**. *Bloomberg Business*. May 16. Accessed online February 7, 2015 at: <http://www.bloomberg.com/news/articles/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour>.

Bradley, T. (2011). **Lessons learned from the Epsilon data breach**. *PCWorld*. April 7. Accessed online June 14, 2015 at http://www.pcworld.com/article/224615/lessons_learned_from_the_epsilon_data_breach.html.

Cachon, G.P., & Fisher, M. (2000) **Supply chain inventory management and the value of shared information**. *Management Science*. 46(8):1032-1048

Cheng, Z., & Nault, B.R. (2012) **Relative industry concentration and customer-driven IT spillovers**. *Information Systems Research*. 23(2): 340-355

Cleeren, K., Dekimpe, M.G., & Helsen, K. (2008) **Weathering product-harm crises**. *Journal of the Academy of Marketing Science*. 36: 262-270

Dyer, J.H., & Singh, H. (1998) **The relational view: Cooperative strategy and sources of interorganizational competitive advantage.** *The Academy of Management Review.* 23(4): 660-679

Gal-Or, E., & Ghose, A. (2005). **The economic incentives for sharing security information.** *Information Systems Research.* 16(2): 186-208.

Gnyawali, D. R., & Madhavan, R. (2001). **Cooperative networks and competitive dynamics: A structural embeddedness perspective.** *Academy of Management Review.* 26(3): 431-445.

Gordon, L.A., Loeb, M.P., & Luchyshyn, W. (2003) **Sharing information on computer systems security: An economic analysis.** *Journal of Accounting and Public Policy.* 22: 461-485

Ha, A. Y., & Tong, S. (2008). **Contracting and information sharing under supply chain competition.** *Management Science.* 54(4): 701-715.

Hausken, K., (2006) **Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability.** *Information Systems Frontiers.* 8: 338-349

Hee-jin, K. (2011). **Nation's worst hacking attack came from China.** *Korea Joongang Daily.* August 12. Accessed on June 14, 2015 at <http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2940129>.

Horowitz, M. (2011) **Spear Phishing: the real danger behind the Epsilon data breach.** *Computer World.* April 7. Accessed online June 14, 2015 at

<http://www.computerworld.com/article/2471050/e-commerce/spear-phishing--the-real-danger-behind-the-epsilon-data-breach.html>.

Hyung-eun, K. (2011) **ESTsoft was ‘host’ of massive cyber caper**. *Korea Joongang Daily*.

August 6. Accessed on June 14, 2015 at

<http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2939860>.

Kelle, P., & Akbulut, A. (2005) **The role of ERP tools in supply chain information sharing, cooperation, and cost optimization**. *International Journal of Production Economics* 93-94: 41-52

Kolfal, B., Patterson, R. A., & Yeo, M. L. (2013). **Market Impact on IT Security Spending**. *Decision Sciences*. 44(3): 517-556.

Kosner, A. W. (2012). **Amazon Cloud Goes Down Friday Night, Taking Netflix, Instagram And Pinterest With It**. *Forbes*. June 30. Accessed online February 7, 2015 at:

<http://www.forbes.com/sites/anthonykosner/2012/06/30/amazon-cloud-goes-down-friday-night-taking-netflix-instagram-and-pinterest-with-it/>.

Liu, D., Ji, Y., & Mookerjee, V. (2011). **Knowledge sharing and investment decisions in information security**. *Decision Support Systems*. 52(1): 95-107.

Ojala, M., & Hallikas, J. (2006) **Investment decision-making in supplier networks:**

Management of risk. *International Journal of Production Economics*. 104: 201-213

Parmigiani, A., Klassen, R.D., & Russo, M.V. (2011) **Efficiency meets accountability: Performance implications of supply chain configuration, control, and capabilities.** *Journal of Operations Management*. 29: 212-223

Schwartz, M.J. (2011). **Epsilon fell to spear-phishing attack.** *InformationWeek DARKReading*. April 11. Accessed online June 14, 2015 at <http://www.darkreading.com/attacks-and-breaches/epsilon-fell-to-spear-phishing-attack/d/d-id/1097119>.

Tallon, P.P. (2011) **Value chain linkages and the spillover effects of strategic information technology alignment: A process-level view.** *Journal of Management Information Systems*. 28(3): 9-44

The Register (2011) **Software maker fingered in Korean hackocalypse.** *The Register*. August 12. Accessed online June 14, 2015 at http://www.theregister.co.uk/2011/08/12/estsoft_korean_megahack/.

Tsung, F. (2000) **Impact of information sharing on statistical quality control.** *IEEE Transactions on Systems, Man, & Cybernetics - Part A: Systems and Humans*. 30(2):211-216

Wagner, S.M., & Bode, C. (2014) **Supplier relationship-specific investments and the role of safeguards for supplier innovation sharing.** *Journal of Operations Management*. 32:65-78

Wang, E.T.G, & Seidmann, A. (1995) **Electronic Data Interchange: Competitive Externalities and Strategic Implementation Policies.** *Management Science*. 41(3): 401-418

Wu, Y., Feng, G., Wang, N., & Liang, H. (2015) **Game of information security investment: Impact of attack types and network vulnerability.** *Expert Systems with Applications.* 42: 6132-3146

Zhou, H., & Benton Jr., W.C. (2007) **Supply chain practice and information sharing.** *Journal of Operations Management.* 25: 1348-1365