Information Security Investment Strategies in Supply Chain Firms: Interplay Between Breach Propagation, Shared Information Assets and Chain Topology

Tridib Bandyopadhyay  
University of Texas at Dallas, tridib@utdallas.edu

Varghese S. Jacob  
University of Texas at Dallas, vjacob@utdallas.edu

Srinivasan Raghunathan  
University of Texas at Dallas, sraghu@utdallas.edu

Follow this and additional works at: https://aisel.aisnet.org/amcis2005

Recommended Citation
https://aisel.aisnet.org/amcis2005/456

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2005 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Information Security Investment Strategies in Supply Chain Firms: Interplay between Breach Propagation, Shared Information Assets and Chain Topology

Tridib Bandyopadhyay  
The University of Texas at Dallas  
tridib@utdallas.edu

Varghese S Jacob  
The University of Texas at Dallas  
vjacob@utdallas.edu

Srinivasan Raghunathan  
The University of Texas at Dallas  
sraghu@utdallas.edu

ABSTRACT
Firms in a supply chain share information assets among them, and make use of inter-firm network connections to enable quick information sharing. Both of these approaches have significant implications when a security breach occurs. One, the interconnections may become conduits for security breach propagation. Two, shared information assets now become vulnerable at the owner as well as at the partner firms’ sites. Therefore, an effective security investment strategy in a supply chain must take into account vulnerability issues arising out of propagation of security breaches and sharing of information assets. Investments in perimeter security technologies reduce direct vulnerability of information assets, but are ineffective in countering indirect breaches, which originate from partnering firms. Our research investigates interdependent security investment strategies of supply chain firms in a game-theoretic framework, and analyze non-cooperative and centrally administered investment equilibria. We also provide comparative static of these investments under specific value chain topologies.

Keywords  

INTRODUCTION
Supply chains have enabled partnering firms to operate with enhanced quality, added flexibility and increased efficiency in business efforts. A key reason for this is the advances in information and communication technologies that have made the flow of information between the firms in the supply chain almost effortless. Today supply chain firms employ various communications (EDI, VPN etc.) and other information technologies (DDBMS, OLAP, ERP etc.) to support their physical flow of goods and services.

When firms employ communication technologies between them, their networks get effectively interconnected. Although network interconnections provide operational benefits to the firms, they impose (added) information security vulnerabilities too. The added vulnerability from probable breach propagation through network interconnections is of significant concern because 1) compromising attacks apparently originate from a friendly (partnering) firm; making it challenging to distinguish between a bona fide and a rogue user, 2) a hacker is motivated to progressively attack more firms in the same chain because of the availability of substitutable and complementary information assets, which greatly increase his/her payoffs, and 3) network interconnectivity among supply chain firms often bypasses security firewalls. In effect, mutual interconnections impose non trivial security vulnerabilities on partnering firms (Ogut, Raghunathan, Menon, 2004).

Supply chain firms also share their information assets (e.g. manufacturers share their production schedule with the suppliers, retailers share their demand profiles with their vendors, etc.) for better customer service, and other competitive and strategic gains. This makes a shared information asset vulnerable not only at the owner firm but also at the partnering firms, with whom the asset has been shared. Distinguishing aspects of this vulnerability are the following: 1) they arise independent of the existence of mutual interconnections; 2) resulting loss exposures are distributed at locations (firms) where the owner firm has little or no influence in terms of security practices and management interventions; 3) loss exposures may duplicate at several locations (the retailer might share a sanitized dataset of consumer demand with several vendors).
Together, use of modern communication and data transfer technologies, and information asset sharing practices among supply chain firms give rise to complex information security risks on two dimensions: 1) risks arising out of ‘network connectivity’, and 2) risks arising out of ‘shared information assets’. Proper appreciation of both of these dimensions is imperative to ensure a complete characterization of interdependent security problems of a supply chain firm (Bandyopadhyay, Jacob, Ragunathan, 2004).

![Information Interdependence and its Dimensions]

In this paper we address the following question: - ‘Facing information security risks along the two dimensions, network interconnectivity and shared information assets, how should supply chain firms invest in security technologies? Our research investigates the interdependent investment strategies of firms in a supply chain with in a game theoretic framework. Specifically, this work studies equilibrium and off-equilibrium investments of supply chain firms in perimeter security under hub and spoke, and value constellation topologies. Interestingly, our analysis corroborates the observed leadership of large retailers in hub and spoke arrangements strictly from an information risk perspective. This research also indicates why vendors in a hub and spoke supply chain are likely to be more responsive to changes in breach propagation risks than the retailer.

Our research contribution is two-fold. We believe this is the first time an effort has been made to link information security investment issues with that of supply chain topologies. But more importantly, this research indicates how information asset sharing and security investment decisions are intimately related in a supply chain. This has important managerial implications - suggesting why security investment decisions need be designed into information asset sharing strategies.

The rest of the paper is organized as follows. Section 2 provides a brief literature review. Section 3 provides a generalized treatment of distributed loss exposure in an N-firm supply chain and argues for topology specific analysis. Section 4 explains our model background, asset sharing arrangements, and nature of loss exposure before listing model assumptions and notation. Section 5 introduces the model under hub and spoke, and value constellation scenarios to analyze interdependent security investment strategies of supply chain firms. Section 6 recapitulates the high points, indicates our future research, and discusses managerial implications of the work.

LITERATURE REVIEW


However, In contrast to previous research, we investigate the combined effect of asset sharing and network connectivity on the security investment in a supply chain under practical supply chain topologies. The integration of the topology issue is significant because this 1) characterizes a real life business scenario and 2) captures supply chain firm behavior in presence of network connectivity.
N-FIRM SUPPLY CHAIN

The general analysis of N-firm supply chain is burdened by the exploding number of possible combinations of interconnectivities among partnering firms, multiplicity of sharing rules among supply chain partners, and the stochastic propagation dynamics of breach/attack. What follows is an indicative treatment only.

Consider $F_i$ to be the $i^{th}$ firm in an $N$-firm supply chain. Define $L_{ij}$ as the (absolute) loss exposure of the $i^{th}$ firm at the $j^{th}$ firm’s network. Thus when a hacker gains access in the supply chain and exploits the existing interconnectivity among the partnering firms, the expected aggregate loss exposure of firm $F_i$ is:

$$E[L_i] = \sum_{j=1}^{N} L_{ij} E[\hat{I}_j]$$

Where the indicator variable $\hat{I}_j$ is defined as follows:

$$\hat{I}_j = \begin{cases} 1 & \text{when firm } F_j \text{ has suffered at least a direct or propagated breach} \\ 0 & \text{otherwise} \end{cases}$$

Noting that the breach propagation may not begin without at least one direct breach, the general expression for the expected value of the indicator variable takes the form:

$$E[I_j] = \sum_{k \in N} \left[ 1 - \prod_{i \in k} (1 - p_i(c_i)) \right] r_{(k)}$$

Where $\langle k \rangle$ stands for the cardinality of the contaminated sub-graph $k$, and $r_{(k)}$ is the probability that the sub-graph $k$ is connected. Also, $p_i(c_i)$ stands for the probability that a firm may be breached when it has invested $c_i$ in perimeter security technologies.

Firm $F_i$ thus minimizes $c_i + E[L_i]$ to arrive at its optimal interdependent security investment level $c_i^*$.

A non-trivial solution of the above requires practicable assumptions for 1) breach propagation dynamics, 2) asset sharing rules, and 3) structural interconnectivities, specific to the institutional scenario of a supply chain. In the following sections we will thus limit the breach propagation only by actual (topology defined) connectivity among the firms, first degree contamination probabilities with respect to every possible propagation path (i.e. propagation may not traverse any link more than once). For the sake of mathematical tractability (without any loss in generality) we will also impose symmetric assumptions among firms in terms of 1) asset sharing arrangements ($L_i = L_j = L, \forall i,j$), 2) technology transfer functions ($TTF_i = TTF_j \forall i,j$), and 3) inter-firm breach propagation probabilities ($q_{ij} = q_{ji} = q, \forall i,j \ i \neq j$): such that equilibrium investment strategies are isolated in terms of 1) topological arrangements of the supply chain, 2) asset sharing intensity, and 3) breach propagation severity.

MODEL BACKGROUND AND PRELIMINARIES

Breach probability and technology transfer function (TTF)

Consider a supply chain firm $F$. Please recall that information interdependence of this firm arises out of existing inter-firm connectivity, and sharing of information assets with other partnering firms (Figure 1).

The firm is also a web enabled business entity, and is exposed to direct breaches from this general environment. $F$ invests $c$ towards its own perimeter security technologies. A firm specific technology transfer function (TTF) maps its investment $c$ to breach probability $p(c)$. Currently available security technologies may not ensure complete immunity from a breach for any finite investments (asymptotic tail of TTF). In absence of investment in perimeter security technologies, an attack is presumed to succeed with certainty ($p(0) = 1$). The TTF (Figure 2) is assumed continuous, at least twice differentiable in its argument, and exhibits decreasing marginal impact of investment. A realized (direct/indirect) breach in firm $F$ could also propagate to a partnering firm (indirect breach) with probability $q$ in case a mutual interconnectivity between them exists. Firm $F_i$’s information assets are thus exposed to direct and indirect breaches at its own, and also at the partnering firms’ networks.
Nature of loss exposure

The distributed loss exposure of a firm arises out of 1) sharing arrangements of information assets and 2) dynamics of attack/breach propagation in the supply chain. Loss exposure, arising out of sharing arrangements of information assets, depends on the ‘type’ of information asset shared. Sharing ‘transactional’ information assets (e.g. an existing VMI system) expose a part of the asset at the owner firm, and the rest at the firm with whom it has been shared. Sharing ‘strategic’ information assets (e.g. sharing sanitized databases) expose the whole worth of the asset at the owner firm but only a part of it at the firm with whom it has been shared. (However, this research considers only transactional asset sharing relationships among the supply chain firms.) Magnitudes, ownerships, and proportions of shared assets depend on alliance defined relationships, and Locations depend on the topology of the supply chain. Dynamics of attack/breach propagation (which translates to inter-firm contamination probabilities) depend on 1) network architecture and topology, 2) security policies and practices and 3) technologies employed. Thus institutional factors and motivations that create a supply chain in the first place, play a major role in the way a breach/attack could trigger and modulate this process in the given topology of a supply chain.

Model assumptions and notation

1) Supply chain topology defines mutual interconnectivities
2) Direct business relationship leads to sharing of information assets, and firms share only transactional assets
3) A breach in to a firm’s network compromises resident information assets
4) An indirect (propagated) breach is strictly conditional upon a direct breach at the originating firm’s network
5) Investment in perimeter security technologies does not affect (indirect) breach propagation
6) Firms’ utility functions are linear in their argument

| $c_i$ | Investment of firm $F_i$ in perimeter security technology, $i \in \{r,v\}$, $c_i \geq 0$ |
| $p_i$ | Probability of a direct security breach in firm $F_i$, $p_i(0) = 1, p_i(c_i) \leq 0, p_i(c_i) \geq 0$ |
| $q$ | Probability of a security lapse causing indirect breach between two adjacent firms, $0 \leq q \leq 1$ |
| $\alpha_i$ | Firm $F_i$’s fractional loss when its information asset is breached at its own network only, $0 \leq \alpha \leq 1$ |
| $L_i$ | Total absolute loss exposure of firm $F_i$. |

Table 1. Model notation
Illustration of shared information assets and loss exposure (2 firm case)

Before we present our model in specific supply chain scenarios, we illustrate sharing of information assets, and the absolute loss exposures; when the number of firms is limited to 2. Please note that the expected loss exposure is modified by the effective (direct and indirect) breach probabilities at the depicted firms.

THE MODEL – HUB AND SPOKE ARRANGEMENT

Consider a supply chain of a retailer (subscript r) and several of its vendors (subscript v), as in the following illustration, \( N = \) total number of firms. The retailer enjoys an effective freedom of \( (1 - p_r)(1 - p_v)^{N-1} \) from any breach, such that the probability that it suffers at least one direct or indirect breach is \( 1 - (1 - p_r)(1 - p_v)^{N-1} \). The probability that a vendor suffers at least one direct or indirect breach is given by \( 1 - (1 - q p_r)(1 - q p_v)(1 - q^2 p_v)^{N-2} \). Please note that we implicitly assume a total of \( N-1 \) simultaneous random draws when a breach is about to propagate to a vendor, originating either from the retailer or from one of the remaining \( N-2 \) vendors.
The retailer’s problem

The retailer has an exposure of $\alpha L$ at its own network, and the rest is symmetrically distributed among all other vendor firms, such that the retailer solves the following problem:

$$
\max_{c_r} \left( -c_r - \alpha L [(1-(1-p_r)(1-q p_v))^{N-1} - (1-\alpha)L (1-(1-p_r)(1-q^2 p_v))^{N-2} \right)
$$

The first term in the above expression represents the retailer’s investment in security technologies; the second term represents its expected loss exposure at its own network; and the third, its expected aggregate loss exposure over all the vendor firms. (Symmetric conditions $\alpha_r = \alpha, L_r = L_{imposed}$)

The FOC of above yields:

$$
p_r' = -1/L \left[ \alpha (1-q p_v)^{N-1} + q(1-\alpha)(1-p_r)(1-q^2 p_v)^{N-2} \right]
$$

Thus the simultaneous Nash equilibrium investment of the retailer is given by

$$
p_r' (c_r^*) = -1/L \left[ \alpha (1-q p(c_r^*))^{N-1} + q(1-\alpha)(1-p(c_r^*))(1-q^2 p(c_r^*))^{N-2} \right] \quad \text{(R)}
$$

Please note that the vendors’ reaction functions in expression (R) have been replaced by their respective (symmetric) equilibrium values of interdependent security investments.

The vendor’s problem

A vendor firm, on the other hand, solves the following problem simultaneously with all other vendors:

$$
\max_{c_v} \left( -c_v - \alpha L [(1-(1-p_r)(1-q p_v))^{N-2} - (1-\alpha)L (1-(1-p_r)(1-q^2 p_v))^{N-2} \right)
$$

As again, the first term in the above expression is the security investment of a vendor firm, the second term is its expected loss exposure at its own network, and the third term represents its expected loss exposure at the retailer firm, with which it shares its information assets. Please note that we have separated an arbitrary vendor firm, subscript 1, in order to investigate its investment decision, which is identically equal to any other vendor firm in the chain. Also, by our problem assumption, there is no asset sharing relationship among vendors themselves. (Also, symmetric conditions $\alpha_v = \alpha, L_v = L_{imposed}$)

Thus, the simultaneous Nash equilibrium investment of a vendor firm is:

$$
p_v' (c_v^*) = -1/L \left[ \alpha (1-q p(c_v^*))^{N-1} + q(1-\alpha)(1-p(c_v^*))(1-q^2 p(c_v^*))^{N-2} \right] \quad \text{(V)}
$$

Binomially expanding, and then dropping higher order terms involving products of $p$ and $q$ (practical values of these parameters are quite low) of order 3 and above, the implicit investment strategies of the retailer and the vendors simplify to:

$$
p_r' (c_r^*) = -1/L \left[ \alpha + q (1-\alpha - p(c_r^*)) - \alpha q (N-2)p(c_r^*) \right] \quad \text{(R)}
$$

$$
p_v' (c_v^*) = -1/L \left[ \alpha (1-q) + q(1-p(c_v^*)) \right] \quad \text{(V)}
$$

![Figure 5. Implicit Location of Optimal Investment](image-url)
Two important observations are in order now. First, pending a specific functional form of the TTF of the supply chain firms, expressions \((r)\) and \((v)\) implicitly locate the equilibrium security investment of the retailer and the vendor on the investment axis, the general nature of which is depicted in Figure 5. Second, conveniently note that the equilibrium investment \(c_r^* (c_v^*)\) and the denominators of expressions \((r)\) and \((v)\), denoted as \(D_r^*\) and \(D_v^*\) (defined below) move in the same direction.

\[
[\alpha + q(1 - \alpha - p(c_v^*)) - \alpha q(N - 2)p(c_v^*)] = D_r^*, \quad \alpha(1 - q) + q(1 - p(c_v^*)) = D_v^*
\]

**Proposition - 1**

In a symmetric supply chain with hub and spoke arrangement of retailer and its vendors, equilibrium investment in interdependent security of a vendor is higher than that of the retailer.

**Proof:** Expression \((r)\) / Expression \((v)\) suggests the following:

If \(q(p(c_r^*) - p(c_v^*)) > \alpha(\alpha + p(c_v^*)[1 + q(N - 2)])\), then the equilibrium investment of the retailer lies right of the equilibrium investment of the vendor on the investment axis (Figure 5), which also necessarily implies \(p(c_r^*) < p(c_v^*)\).

However, this is a contradiction because when \(p(c_r^*) < p(c_v^*)\), the LHS of the above expression is negative, and necessarily smaller than the RHS, which is always positive. By the same argument, \(c_r^*\) and \(c_v^*\) may not even be coincident on the investment axis for any supply chain with \(N \geq 2\), because by the current state of security technology, complete immunity from breach is unattainable ( \(p(c_v^*) > 0\) ), even though firms may agree to share all of its information assets \((\alpha = 0)\). Lastly, \(N < 2\) is an absurdity by definition of a supply chain. Q.E.D.

The above result is suggestive of the fact that under current topological scenario of hub and spoke, and the given asset sharing arrangements, the retailer has a net advantage of risk diversification. Although sharing exposes information assets to direct breach at the shared firms, multiplicity of sharing relationships with the vendors (none of whom invests less than the retailer at equilibrium), gives this unique advantage to the retailer. Ceteris paribus, the retailer thus exhibits lower propensity towards security technology investments at the Nash equilibrium. On the other hand, the vendors have unary relationship with the retailer alone, and may not diversify their risks of exposure. Interestingly, proposition-1 corroborates the standard prudence in risk management - that a well diversified portfolio of assets begets reduced loss exposure.

It is of great interest to investigate the investment adjustments made by the retailer and the vendors at the equilibrium levels, when breach propagation probability \(q\) or sharing proportions \((\alpha)\) are perturbed. This is so, because supply chain firms do redefine their associations \((\alpha)\) with the partnering firms over time, and firm specific factors (changes in employee morale, integrity, turnover, etc.) affect inter-firm breach propagation probability \(q\) over time.

**Proposition - 2**

As propagation probability \(q\) increases, the threshold at which the vendor begins to respond with increasing security investment is never higher than that of the retailer. This difference of the thresholds becomes more pronounced as the supply chain increases in size.

**Proof:** Recalling from page 11, we have

\[
D_r^* = \alpha + q(1 - \alpha - p(c_v^*)) - \alpha q(N - 2)p(c_v^*), \quad \text{and} \quad D_v^* = \alpha(1 - q) + q(1 - p(c_v^*)), \quad \text{such that}
\]

\[
D_r^* (q) = (1 - \alpha)(1 - p(c_v^*)) - \alpha(N - 1)p(c_v^*)\] and \(D_v^* (q) = 1 - \alpha - p(c_v^*)\)

Noting that \(c_v^*\) and \(D^*\) (with either of the subscripts) move in the same direction, we can infer that for small increases in propagation breach probability \(q\), the equilibrium investment of the retailer could increase only if \(c_v^* < p^{-1}(1 - \alpha)\), and the same of the vendor could increase only if \(c_v^* < p^{-1}(1 - \alpha)\) (Figure 6), such that the threshold for retailer is higher than that of the vendor \(\forall N > 2\). Also, as \(N\) increases, the threshold for the retailer, \(p^{-1}(1 - \alpha)\), remains unchanged; such that the difference of thresholds increases with the number of firms in the chain. For \(N = 2\), the thresholds are trivially same as can be expected in a symmetric firm analysis; - there remains no factor which could distinguish the retailer from the vendor in a 2 firm chain. Q.E.D.
Figure 6. Thresholds for increasing investments by the retailer and the vendors

Figure 6 above graphically explains proposition 2. An agreed level of information assets sharing ($\alpha$), defines a pair of planes $RR$ and $VV$. Depending on the initial levels of security investments made by the supply chain firms, reactive adjustments are made when the contamination (propagation) probability $q$ changes over time. For small increases in $q$, the retailer increases its investment only when the vendors’ investments lie towards right of the vertical plane $VV$. On the other hand, under increasing conditions in $q$, vendors increase their investment so long the retailer’s investment falls towards right of the vertical plane $RR$. (Towards the left of the aforesaid planes, negative externality in security investment takes over for the other party, as probability of breach propagation $q$ increases). The horizontal distance between the planes $RR$ and $VV$ is the difference between the thresholds. Note that as the number of firms increase in the supply chain, the distance between $RR$ and $VV$ is poised to increase.

When sharing increases, i.e. $\alpha$ falls, $RR$ and $VV$ both move leftwards, but $VV$ moves at a higher rate than $RR$, such that the difference in the thresholds reduces faster than the rate at which sharing increases. This happens as a combination of the following factors. 1) For chains with $N > 2$, with decreasing $\alpha$, $(1-\alpha)^{\frac{1}{1+\alpha(N-2)}}$ rises faster than $(1-\alpha)$ on the $Y$ (breach probability) axis. 2) The increased flatness of the TTF at higher investments causes $VV$ to move faster on the $X$ (investment) axis.

When proportionally higher ratio of retailer’s (vendor’s) assets rest at the vendor’s (retailer’s) network, the retailer (vendor) is increasingly interested to have the vendor (retailer) increase its investments in security. Under symmetric Nash equilibrium, the only way a retailer (vendor) may elicit this desired behavior is by investing more in its own network, and be towards right of the plane $RR$ ($VV$). The relative position of $RR$ makes it much easier for the retailer to exhibit this expected behavior in a supply chain.

In other words, because it can respond and handle the increased security risk that is associated with an increase in information asset sharing arrangements at a relatively lower level of investment, a retailer in a hub and spoke arrangement is expected to be in favor of employing more shared information assets and systems, as is commonly observed in large retailers in reality\(^1\). This apparent ease to exhibit an expected behavior in the business relationship also explains in part the natural leadership structure that we observe in large hub-and-spoke supply chains.

\(^{1}\) For example, Wal-Mart’s apparent enthusiasm in employing RFID systems.
Proposition - 3

As vendors share more of their information assets with the retailer, their equilibrium investment in security technologies decreases irrespective of the size of the supply chain so long breach propagation is not a certainty. When retailer shares more of its information assets with the vendors, its equilibrium investment in security technologies may not increase unless the chain is very small.

Proof: The first part of the proposition is apparent from $D_v^s \alpha = 1 - q$, such that for $q < 1$, as sharing increases (decrease in $\alpha$), $c_v^*$ falls.

Next, from $D_v^s \alpha = 1 - q[1 + (N - 2)p(c_v^*)]$, increased sharing by the retailer may result in higher level of own equilibrium investment only when the precondition $c_v^* < p^{-1}(1-q/q(N-2))$ is met. Under symmetric Nash equilibrium, when retailer increases sharing, vendors must identically respond by increasing their sharing proportions. This has a tendency to decrease vendors’ investment in security technologies (first part of proposition 3) which makes the above precondition increasingly unattainable. Q.E.D.

Proposition 3 implies that for large chains, as retailer shares more, the effective benefit (in the face of reducing equilibrium level of investment by the vendors, by symmetric Nash assumptions) of increasing own investment is greatly diluted. Hence is the result.

Value constellation

We define value constellation as a group of interdependent firms who transact business among themselves on a near-equal footing, such that each member of the constellation maintains direct connectivity and asset sharing relationship with every other firm. Structurally, a value constellation is equivalent to a fully connected network of firms. It can be shown that the simultaneous Nash equilibrium of interdependent security investment of any of the firms in a value constellation essentially yields the same insights as we have garnered in case of the retailer in the hub and spoke arrangement. In the previous section, the retailer was distinguished by the way a breach from it could reach any other firm in one single hop (and vice versa), and multiplicity of asset sharing relationships, which is true for every firm in a value constellation.

However, given the asymmetric power structure of a retail chain, a social solution for the interdependent security investment problem is of little practical significance there. On the other hand, a value constellation is rather apt to engage in a central approach for their interdependent security investment decision problem. We thus discuss the social solution of the problem here with our usual symmetric assumptions in state.

A social planner would like a firm to minimize the total expected loss exposure of the constellation at its site rather than its own parochial loss exposure alone. This characterization yields the following problem for $F$ to solve:

$$\max_{c_i} \left( -c_i - L(1- (1-p))(1-qp)^{N-1} - (N-1)L(1- (1-qp))(1-p)(1-qp)^{N-2} \right)$$

The first term is firm $F_i$’s investment, the second is the total expected loss exposure of all assets at $F_i$’s site and the third is its remaining aggregate expected loss exposure at all other firms. As before, we have separated an arbitrary firm $F_i$ so as to be able to isolate firm specific investment decision $c_i^*$ at equilibrium.

The FOC of the above yields:

$$p_i^* = -1/L/(1-pq)^{N-1} + q(N-1)(1-p)(1-pq)^{N-2}$$

Realizing that every firm will behave identically at equilibrium, the optimal solution is now given by:

$$p_i^*(c^*) = -1/L/(1-qp(c^*))^{N-1} + q(N-1)(1-p(c^*))(1-qp(c^*))^{N-2}$$

Interestingly, the equilibrium investment no longer depends upon the sharing intensity because each firm is now responsible for a symmetric share of everyone’s asset. Expanding binomially, and dropping higher order terms for small values of $p$ and $q$, the above relationship reduces to $p_i^*(c^*) = -1/L/(1-q(N-1)(1- p(c^*)))$, which implies that as the number of firms increase in a value constellation, the equilibrium level of investment decreases among the constituent firms. This happens because now each firm must consider the total exposure at its own site, and under symmetric assumption, the net effect of shared information assets ceases to exist.
In absence of the effect of shared information assets, investment decisions in the value constellation is governed by network connectivity issues alone, and exhibits decreasing investment in the face of increasing breach probability (echoes finding of Ogut et al., 2004). 

\[ D^*(q) = -(N-1)(1-p(e^*)) \]

**CONCLUSION**

We argue that 1) a shared information asset is vulnerable at its owner’s, and at all of the sharing firms’ networks and 2) an information asset (shared or not) is vulnerable at the owner’s network from direct and propagated breaches. Exploring the general N-firm case, we 1) identify modeling issues for studying interdependent security investment strategies of value chain firms and 2) rationalize our simplifying assumptions. Isolating the hub and spoke arrangement, we explain 1) how network externality may affect interdependent security investment strategies, 2) why the retailer is likely to enjoy a favorable leadership profile, 3) how the retailer’s risks are so diversified and why it may enjoy a lower level of security investment, and 4) why the vendors may exhibit higher propensity towards adjusting their equilibrium levels of investment, when faced with changing profile of breach propagation. In a changed scenario, where firms are in a value constellation, we derive the social solution, and explain why negative network externality in security investment may be the order of the game.

Our work brings out important insights: 1) Past decisions on information asset sharing intensity (a) affect today’s efficient level of investment in security technologies (c*) in supply chain firms, 2) increased size of chain widens the gap of investment thresholds between the vendors and the retailer, when contamination probability rises. Together, these have important business connotation: 1) firms need to integrate security considerations during information sharing decisions itself and 2) chain expansion moderates investment behavior of all constituent firms. Our research also explains the observed leadership role of the retailer in a hub and spoke arrangement purely from an angle of distribution of risks and ease of risk mitigation.

This is an ongoing project, and our future efforts include 1) solving the model for other supply chain topologies including the manufacturer – supplier concatenation arrangement and 2) designing mechanisms for desirable levels of interdependent security investment in presence of security preferences and other asset sharing rules. This work leads us to conjecture that sharing and investment decisions may be best taken up in separate phases as a chain grows to maturity, and is an important direction that this research may be extended.

**ACKNOWLEDGEMENT**

This research has been supported in part by International Center for Decision and Risk analysis (ICDRiA), School of Management, The University of Texas at Dallas.

**REFERENCES**