8-5-2011

IT Security in Supply Chain: Does a Leader-Follower Structure matter?

Tridib Bandyopadhyay
Kennesaw State University, tbandyop@kennesaw.edu

IT Security in Supply Chain: Does a Leader-Follower Structure matter?

Tridib Bandyopadhyay
Kennesaw State University
tbandyop@kennesaw.edu

ABSTRACT

Using a traditional leader-follower decisional sequence as the manifestation of power structure in a supply chain, this work generalizes extant research in IT security. We propose a game theoretic model to analyze the equilibrium IT security of the supply chain in the Stackelberg game, where the power structure in the supply chain manifests in a natural leader. Our results indicate that a natural leader-follower framework ensures higher IT security in the chain than the decentralized decision scenario. However, our results also exhibit that the total cost of IT security is disproportionately divided between the firms of the supply chain. In equilibrium, the leader not only commits first, it must also commit at a higher level than the follower. General comparison with the centralized case as well as the sensitivity of IT security investment of the leader/follower firm on key network parameters is also analyzed.

Keywords

Supply chain, IT security, supply chain security, interdependent IT security risk, cyber risk, business process integration risk.

INTRODUCTION

The business world is more networked now than ever. This creates the possibility that a breach from one firm could propagate to another with the help of the facilities and interfaces of firms which run on the Internet. As a result, IT security risks of modern firms are now interdependent on one another. Research indicates that collaboration between firms in IT security, for example: sharing breach information with or without the help of a centrally coordinating agency (Gal-Or et. al. 2005), has desirable outcomes in today's networked world. The above observations are general, and apply to firms who utilize the Internet as one of the enablement/channels in their business operations.

For firms in a supply chain (henceforth ***SC***) - where collaborative relationship preexists in the operational front in terms of integrated business processes, - interdependence in IT security has additional connotations. Since business process integration requires that the SC firms share and cross utilize their information assets and networks with one another, a breach to one firm gives rise to loss not only to the breached firm but also to the other firms in the SC. In other words, irrespective of whether the breach progressively propagates to the other firms in the SC or not, a breach can still incur indirect loss to multiple firms in the SC. Consequently, business process integration and IT security decisions become jointly interdependent between the firms in a SC (Bandyopadhyay et. al., 2010). However, collaboration between the firms in a SC still retains the earlier advantages and maintains a lower overall cost of IT security for the firms in a supply chain.

However, collaboration in IT security between SC firms is a scantly researched area that needs further investigation. General market observation suggests that not all firms in a SC may enjoy the same decisional power. Literature provides reasons and structures of unequal decisional power between the firms in a SC (e.g., Mukhtar et. al. 2002). Relative sizes of the firms, tenure of collaboration in the SC, market structure, topological factors, price/process leadership and technological prowess, among others, are the causes that create unequal power status between the firms in a SC. It is thus logical to expect that firms may not be able to exercise equal decisional power even in the realm of collaboration in IT security. For an extreme example, consider the case of Wal-Mart. A firm, that desires to join the suppliers' network of Wal-Mart, must first comply with the IT security requirements specified by Wal-Mart before they are allowed to do any business with Wal-Mart (www.walmart.com/smalbusiness). It is reasonable to expect that collaborative IT security decisions in a SC are likely to be taken in the context of preexisting operational relationships, including the power structure, when one exists.

One interesting question to ask at this point is how power structure affects IT security decisions in the context of partnering firms in a supply chain. In this research we attempt to address the above general question. Specifically, we consider a leader-follower sequence in the IT security decisions as the manifestation of an existing power structure in the SC, and propose a model to analyze and qualify the IT security decisions in a supply chain. We have initial results which lead to significant

managerial implications. We first show that IT security of a supply chain is improved in general when one firm takes the lead and invests first in IT security, compared to the case where both firms take simultaneous decisions individually. Next, we show that the leader pays dearly for its initiative - in equilibrium, the leader incurs higher overall IT security cost than the follower. We also exhibit how network vulnerability of the supply chain further impacts the costs of IT security of the leader/follower firms. In order to keep the analytical model tractable, our model considers a simple SC with two symmetric firms; yet brings out significant managerial insights about the IT security decisions for firms in a supply chain.

The rest of the paper is as follows. First we provide a brief survey of the relevant literature. Next, we characterize the interdependent IT security risk between the firms in a SC and propose our model. Having done so, we then analyze the model and compare the investment decisions of the constituent firms under **3** different decision scenarios: *first*, when the firms take their independent decisions simultaneously, *second*, when a centralized decision maker takes simultaneous decisions for both the firms, and *third*, when one firm takes the lead and makes its independent decision which is then followed by the other firm, who has earlier observed the decision of the leader.

LITERATURE REVIEW

This work comes in the interface of process and business integration that manifest in supply and value chain, their IT enablement and the attendant risks. We thus review literature that covers value proposition of IT enablement of supply/value chain, and IT security, including supply chain security.

Several studies concentrate on EDI system between firms, although the more recent ones consider open systems based on the Internet. Srinivasan, Kekre and Mukhopadhyay (1994) have identified EDI and distributed databases as major IT enablers of overall performance in supply chain. Brousseau (1994) and Dearing (1995) find reduction in transaction costs, and finds that the source of the benefits comes from the savings in procurement and monitoring expenses. Kekre and Mukhopadhyay (1992) infer that EDI may reduce inventory while increasing product quality. Wang and Seidman (1995) exhibit positive externalities for the participants and negative externalities for non-participants in an EDI based supply chain network. Dearing, in a later work (1995) argues that EDI deployment helps shorten lead times, which is supported by Niederman (1998). Lim and Palvi (2000) provide empirical evidences of strong relationship between EDI and customer performance. Susarla, Barua, and Whinston (2007) utilize survey methodology to find that information integration and coordination results in positive impact on efficiency of SC.

The role of the Internet in supply chain management has been studied by Smith and Oliva (2000). Kambil et al. (1999), Croom (2000) study the Internet mediated standardized transacting procedures which are shared by many firms. Kaplan and Sawhney (2000) identify that Internet procurement reduces transaction costs and increases competition in procurement process. Hagel III and Singer (1999) find that infomediaries, who aggregate buyers and suppliers with open architecture of connection and standardized transactions; inducing horizontal, pooled interdependencies among buyers and suppliers. Continuous replenishment enabled by EDI has been studied by Cachon and Fisher (1997), who establish positive benefits for EDI implementation at Campbell Soup.

In one of the original studies in IT security, Varian (2002) analyzes the IT security investment of an information system that connects multiple firms, and shows existence of free rider problems. In his model, IT security is treated as a common public good between the connected firms, who must provide for the resources for the security of the interconnected system by private contributions. Kunreuther and Heal (2003) show when firms' risks are interdependent, then two conditions arise in equilibrium: a) either all firms or b) no firm invest in security. Tanaka et al. (2005) empirically verify the relationship between vulnerability of IT system and information security investment of firms, which were originally predicted by Gordon and Loeb (2002). Ogut et al. (2004) investigate interdependency on firms' investment in IT security between the technological controls and financial instruments. Hausken (2006) analyze the combined impact of interdependence, income, and substitution effects on interconnected firms' security investments. One important stream of research considers the impact of information sharing, e.g. breach information, vulnerability and patch update information etc. as impacting the IT security health of firms. Gordon, Loeb, and Lucyshyn (2003) show that when firms share security information, firms' incentive to invest in information security reduces. On the other hand, Gal-Or and Ghose (2005) exhibit that under certain consideration, security information sharing and security technology investments may work out to be mutually strategic complements! In a later work, Hausken (2007) recalculates firm's incentive in IT security investment with additional assumptions that allow substitutability between a firm's security investment and information received by the other firm, but allows complementarities, to yield that the interdependence is negative. Bandyopadhyay, Raghunathan and Varghese (2010) investigate firms' incentive in IT security investment in SC under information asset sharing. They show that network vulnerability and information asset tend to have compensating forces, thus exhibiting that both positive and negative network externality in IT security investment in IT security is possible. However, their research considers only simultaneous

investment decisions in IT security by the SC firm, which however we now attempt to extend for the Stackelberg type of game in this research.

MODEL FORMULATION

The subsections are organized in the following manner: *First*, we present our notation. Second, we define the IT security risk interdependence between the SC firms. *Third*, we define the direct and indirect breach that a firm in SC may suffer. *Fourth*, we present the assumed nature of the transfer function that maps IT investment dollar investment into feasibly controlled breach scenario. Fifth, we explain the structuring of losses in the SC firms and specify the model. *Finally*, we present the model that captures the above characterization of IT security problem in the context of supply chain. We consider a 2-firm SC for our modeling purposes, and later simplify it further by imposing symmetric parametric constraints between the firms for tractable analysis.

Notation

c_i	Investment of Firm-*i* in security technology, $c_i \geq 0$
p_i	Probability of a direct breach (follows *TF)*, $p_i(0) = 1, p_i'(c_i) \leq 0, p_i''(c_i) \geq 0$
q_{ij}	Probability of an indirect breach via firm Firm-*i* to Firm-*j*, $0 \leq q_{ij} \leq 1$
L_i	Loss to Firm-*i* when its information asset is breached at its *own* networks only.
${}^i\beta_2 L_i$	Loss to Firm-*i* when its information asset is breached at its *partner's* network only, through a direct breach. $0 \leq {}^i\beta_2 \leq 1$
${}^i\beta_1 L_i$	Loss to Firm-*i* when its information asset is breached at its own network as well as its partner's network through a *propagated* breach. $1 + {}^i\beta_2 \leq {}^i\beta_1$
$(1 + {}^i\beta_2) L_i$	Loss to Firm-*i* when its information asset is breached at its own network as well as its partner's network through separate simultaneous *direct* breaches.

Table 1. Model Parameters and Variables

IT Security Risk Interdependence

When a firm employs information assets for operational and strategic gains, any compromise of these assets imposes loss. Such losses may come in the forms of opportunity costs, lost business and reputation, recovery efforts, legal implications including liability claims. When firms operate in a supply/value chain framework, the information security risks become interdependent in the following manner:

1. Real time communication and business data transfer connectivity between SC firms (e.g., EDI, VPN etc.) support the integrated business processes in a SC. Breach in one firm can propagate to another firm through the connectivity, causing cascaded compromise of interconnected information assets and business processes of multiple firms.

2. The practice of strategic sharing of information assets expose these assets of one firm to direct breaches at the partnering firm's network – thereby multiplying the seats of exposure, where a risk is realized. When a firm is breached, not only its information assets but also those of other SC firms, who have shared their information assets with this firm, are compromised. For instance, when a vendor is provided with the demand pattern by the retailer to help synchronize an agreed VMI (Vendor Managed Inventory) arrangement, a breach into the vendor's server compromises the demand pattern, bringing loss to the retailer[1].

[1] Such losses may be severe for breaches which are primarily motivated by business espionage.

Network interconnectivity and strategic asset sharing may exist independently, and hence the risks of 1 and 2 could exist independently as well. For case 2 above, if there is no logical or physical connectivity between the networks of the firms - for example, the demand pattern is shared in a storage media - there is no scope for a breach to travel from one firm to another. On the other hand, for case 1 above, a propagated breach affects the freshly compromised firm's own assets if there is no strategic sharing or process coupling arrangement between the firms. For example, if both the firms have agreed on VPN tunneled communication for trusted traffic, a breach can probabilistically travel from one firm to another, but the seats of loss are firmly limited at each firm's servers and networks only. Typically though, both the interdependencies as described in 1 and 2 are likely to be present together in most topologies and arrangements of modern supply chain architecture. As a result, it is appropriate to isolate sharing and interconnectivity as independent dimensions to characterize the interdependent IT security risk of a firm in a supply chain relationship.

Types of Breach

If a firm realizes a breach directly from its general Internet environment, we define this as a ***direct*** breach. When such a breach exploits the mutual connectivity to propagate to a second firm, we define that the second firm has suffered an ***indirect*** breach. Clearly, no indirect breach is possible without a direct breach in at least one other firm in the supply chain.

Investment Transfer Function in IT Security

When a firm invests in security technology, a transfer function ***TF*** (Figure 1) maps this investment to the firm's post investment direct breach probability. The composite transfer function takes care of the available technology standard and the firm's capability to utilize IT security technology effectively. In absence of any security investment, an outsider's attack is assumed to succeed with certainty, $p(0)=1$. The ***TF*** falls asymptotically, signifying that available IT security technology does not provide perfect IT security for any finite investments, $p^{-1}(0)\to\infty$.

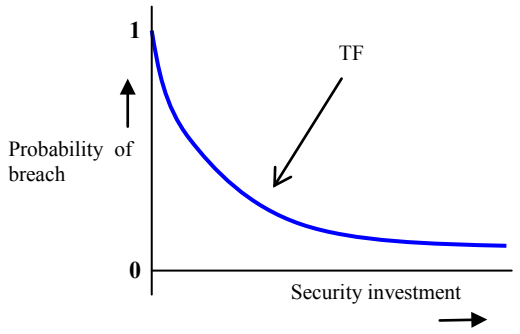

Figure 1. A Firm's Investment Transfer Function in IT security

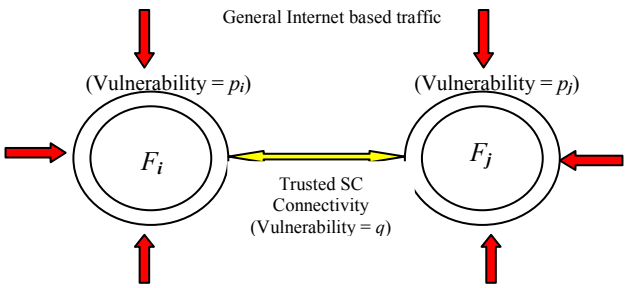

Figure 2. Firms' exposure to IT security risk in SC relationship

Model Specification

Figure-2 depicts the simple two-firm SC that we model in this research. The following paragraph specifies the model and formalizes the assumptions that we utilize to model the SC.

Firm i invests c_i $i\in\{1,2\}$ in IT security. The post investment vulnerability of a direct breach at the perimeter of the firm's Internet connectivity is given by $p_i = p(c_i)$, which is governed by the firm specific ***TF*** (Figure 1). The firms in the SC have a mutual connectivity for inter-firm trusted traffic. However, this link may become the conduit for a hacker to progressively compromise the second firm when s/he has already breached one firm's perimeter security through a direct breach. The link vulnerability q is technology specific and assumed symmetric across the firms in the SC. The business process of the SC is integrated. This requires that each firm shares a part of its information asset ${}^i\beta_2$, $i\in\{1,2\}$, with the other firm $0\le {}^i\beta_2\le 1$.

When only firm i is breached, loss to firm i is L_i. However, firm i also share its information assets with firm j. This shared asset belongs to firm i but resides at firm j's server. As a result, a breach into firm j brings a loss of ${}^i\beta_2 L_i$ to firm i. Loss to firm i when both the firms are simultaneously breached is additive, $\left(1+{}^i\beta_2\right)L_i$. If firm i is breached first, and then the breach

propagates to firm *j*, utilizing the interconnecting link, then the loss to firm *i* is ${}^{i}\beta_1 L_i$. Since business embarrassments including liability issues are additional concerns in such a progressive breach, $1+{}^{i}\beta_2 \le {}^{i}\beta_1$.

Scenarios and Models

Three decision scenarios are captured in this work. These are simultaneous independent (S-1), centralized (S-2) and leader-follower (S-3), which are presented below along with their brief explanations. For consistency, the models are presented from the perspective of firm-1. Firm-2 solves the analogs of the problem, which are similar and not repeated. Note that parametric symmetry in interconnectivity and sharing has already been imposed in the presented models.

Model S-1

$$\underset{C_1}{Max} \quad \left(-c_1 - {}^{1}\beta_1 L_1[p_1(1-p_2)q + p_2(1-p_1)q] - L_1[p_1(1-p_2)(1-q)] - {}^{1}\beta_2 L_1[p_2(1-p_1)(1-q)] - (1+{}^{1}\beta_2)L_1 p_1 p_2\right)$$

The above model depicts the parochial problem that firm-1 attempts to solve in order to arrive at its optimal level of IT security investment. The 1st term in the objective function is F_1's investment in IT security; the 2nd term is the total expected loss to F_1 when both F_1 and F_2 are breached through propagated breach that travels from one firm to the other. The 3rd (4th) term captures the expected loss to F_1 when only F_1 (F_2) is directly breached and the breach does not travel to F_2 (F_1). The 5th term refers to the situation where each of the firms separately suffers direct breaches.

The simultaneous parochial Nash equilibrium investment, c_p^* of a firm in the SC, after imposition of parametric symmetry across firms in the SC yields:

$$c_p^*(\beta, q) = p'^{-1}\left(\frac{-1/L}{1+\beta_1 q\{1-2p(c_p^*)\} + \beta_2 q\, p(c_p^*) - q\{1-p(c_p^*)\}}\right)$$

Model S-2

$$\underset{c_1,\, c_2}{Max} \quad \left[-c_1 - c_2 - 2q\beta_1 L\left(p_1(c_1) + p_2(c_2) - 2p_1(c_1)p_2(c_2)\right) - (1+\beta_2)L\left(p_1(c_1)\{1-p_2(c_2)\}(1-q) + p_2(c_2)\{1-p_1(c_1)\}(1-q) + 2p_1(c_1)p_2(c_2)\right)\right]$$

The above model depicts the optimization problem that the centralized planner attempts to solve. The first 2 terms are the investments made by the firms. The remaining terms together represent the aggregate expected loss between all the different combinations of direct and propagated breaches across both the firms in the SC.

The centralized solution, when parametric symmetry across the firms in the SC is implemented is,

$$c_s^*(\beta, q) = p'^{-1}\left(\frac{-1/L}{2q\beta_1\{1-2p(c_s^*)\} + (1+\beta_2)\left[1-q\{1-2p(c_s^*)\}\right]}\right)$$

Model S-3

The Model S-3 is essentially Model S-1, suitably adjusted for the *leader- follower* structure. Assume that firm-1 leads with investment c_1. Since the follower is able to observe the investment of the leader in our model, firm-1 first calculates the optimal reaction function of firm-2, ${c^{F}}_2^*$, given its own investment c_1, which can be readily arrived from c_p^* above

$${c^{F}}_2^* = p'^{-1}\left(\frac{-1/L}{1+\beta_1 q\{1-2p(c_1)\} + \beta_2 q\, p(c_1) - q\{1-p(c_1)\}}\right)$$

Firm-1 then replaces $p_2 = p(c_2)$ with ${p^{F}}_2^* = p({c^{F}}_2^*)$ in Model S-1 and solves for ${c^{L}}_1^*$, where the superscripts *L* and *F* stand for the leader and the follower in the Stackelberg game, while the subscripts maintain our original designation of the firms.

ANALYSIS

The optimal investments are derivable only in the implicit form, seriously affecting tractability for closed form solutions. We now impose functional form for the IT security investment *TF* of the SC firms, namely $p = p(c) = e^{-k.c}$. Note that this

functional form preserves standard convexity assumptions including reducing marginal impact of IT security investment and offers some tractability, since $p' = -kp$. The closed form solutions of the above models are presented below[2]:

$$c_p^* = p^{-1}\left[\left(\frac{q - q\beta_1 - 1}{2q(1+\beta_2-2\beta_1)}\right) + \frac{\sqrt{L^2K^2(1-q+q\beta_1)^2 + 4LKq(1+\beta_2-2\beta_1)}}{2LKq(1+\beta_2-2\beta_1)}\right]$$

$$c_s^* = p^{-1}\left[\left(\frac{-(2q\beta_1 + (1+\beta_2)(1-q))}{4q(1+\beta_2-2\beta_1)}\right) + \frac{\sqrt{L^2K^2(2q\beta_1 + (1+\beta_2)(1-q))^2 + 8LKq(1+\beta_2-2\beta_1)}}{4LKq(1+\beta_2-2\beta_1)}\right]$$

$$c^{L^*} = p^{-1}\left[\frac{1}{LK\left[\left(1+\beta_2 YZ^*\right) + q\beta_1\left(1+YZ^*-2XZ^*\right) + q\beta_2\left(XZ^*-YZ^*\right) - q(1-XZ^*)\right]}\right] \text{ AND } c^{F^*} = p^{-1}\left[\frac{1}{LK\left(X - Y\,p(c_L^*)\right)}\right]$$

Where $X = 1 + q(\beta_1 - 1)$, $Y = q(2\beta_1 - \beta_2 - 1)$, and $Z^* = 1/\{LK(X - Y\,p(c_L^*))^2\}$.

NUMERICAL ANALYSIS

Although the functional form allows us to derive closed form solutions, further analysis including parametric sensitivities and equilibrium decisions are difficult. Thus we numerically analyze the equilibrium levels of IT security investment of the supply chain firms under the 3 decision scenarios and compare them. The base values utilized for the experiment are $L = 1000,\ \beta_1 = 1.5,\ \beta_2 = 0.2,\ k = 0.01$.

The solution procedure involves solving the optimal investments for each of the three different models utilizing computer software and then calculate the total cost of IT security, defined as the sum of the IT security investment and the post investment expected loss of the firm in the given decision scenario. We repeat the experiment for multiple values of SC relationship parameter, namely the link vulnerability *q*, in order to assess the impact of vulnerability in trusted communication on the equilibrium level of IT security that the firms maintain in a supply chain.

L = 1000, BETA-1 = 1.5, BETA-2 = 0.2, K = 0.01								
	Coordinated Solution		**Simultaneous Solution**		**Stackelberg Leader**		**Stackelberg Follower**	
Link Vulnerability (q)	Investment per firm	Cost per firm	Investment per firm	Cost per firm	Investment	Cost	Investment	Cost
0.10	260.52	359.8654	233.46	365.4225	233.97	365.4212	233.47	365.2686
0.15	266.19	365.3091	235.07	372.7131	235.93	372.7094	235.09	372.4117
0.20	271.63	370.5786	236.67	379.8144	237.93	379.8065	236.71	379.3141
0.25	276.85	375.6717	238.28	386.7307	239.97	386.7162	238.34	385.9790
0.30	281.87	380.5900	239.88	393.4660	242.05	393.4423	239.97	392.4114
0.35	286.70	385.3372	241.47	400.0247	244.14	399.9890	241.61	398.6175
0.40	291.33	389.9188	243.07	406.4113	246.24	406.3604	243.24	404.6048
0.45	295.80	394.3410	244.66	412.6301	248.36	412.5610	244.88	410.3812
0.50	300.10	398.6109	246.24	418.6856	250.47	418.5951	246.51	415.9554
0.55	304.24	402.7353	247.82	424.5824	252.58	424.4675	248.14	421.3360
0.60	308.24	406.7214	249.39	430.3249	254.68	430.1828	249.77	426.5320
0.65	312.09	410.5760	250.95	435.9177	256.77	435.7456	251.39	431.5523
0.70	315.82	414.3060	252.50	441.3651	258.84	441.1606	253.00	436.4055
0.75	319.43	417.9176	254.05	446.6716	260.89	446.4326	254.60	441.1000
0.80	322.92	421.4171	255.58	451.8415	262.92	451.5661	256.20	445.6441

Table 2. Link Vulnerability in SC affecting the equilibrium investment and cost of the constituent firms

[2] The calculations are lengthy, require second order conditions and are not presented here for paucity of space

Observation-1**:** *In order to combat an increased vulnerability in trusted communication, SC firms monotonically increase their equilibrium investment under all decision scenarios*.

The above observation can be explained in the following light. As the link vulnerability increases (for example, open standard technologies instead of EDI are utilized), the perimeter security of firm-2 becomes very important for firm-1, since the cross propagated breaches that affect firm-1 are seeded in firm-2. In the simultaneous parochial game, firm-1 thus invests more, which reduces the cross propagation of breach to firm-2. Benefited, firm-2 reciprocates by increasing its own investment in perimeter security and a higher equilibrium is established. For the Coordinated solution, the central coordinator of course takes a decision that helps all the SC firms who face the increased link vulnerability. Both firms now increase investment in equilibrium under coordinated centralized solution. Similarly, increased link vulnerability cause the leader to increase its own investment and further secure its own perimeter security such that the likelihood of a seeding direct breach is minimized. The follower reciprocates the higher level of security that the additional investment by the leader ushers. In essence, under all decision scenarios, increased link vulnerability is combated with higher investment in perimeter security.

Observation-2**:** *Facing increased link vulnerability, firms face increased cost of IT security in a supply chain relationship*.

First note that an increase in equilibrium investment on the transfer function (TF) moves the quiescent point to a flatter region of the curve. In other words, diminishing marginal return on investment sets in. Now increased investment brings benefits at a decreasing rate, and the rate of fall of equilibrium vulnerability in the perimeter security remains undercompensated in the overall sense in the expected loss of a firm. Finally, the overall cost of IT security - which is really the sum of the increased investment as well as the increased expected loss from higher link and perimeter vulnerabilities - for all the constituents of the supply chain increases. This observation is consistent across all the decision scenarios under consideration here.

Observation-3A**:** *An extant power structure in the SC partially ameliorates the problem of underinvestment in the independent decision scenario. However, a centrally coordinated IT security regime still outperforms the leader-follower equilibrium in terms of the total cost of IT security in a supply chain.*

Observation-3B: *The apparent relative ranking of equilibriums in Observation-3A remains consistent at all levels of link vulnerability that may exist across the firms in a supply chain*.

Observations 3A and 3B are especially significant in terms of managerial relevance. Since expansion of existing B2B relationships including those in the SC arena are continually on the rise, IT managers often face the challenge of integrating an incoming firm's systems with the existing business processes of the SC. This research emphasizes that collaboration in the IT security initiatives across the firms in a chain ensures that the SC may enjoy and benefit from an efficient IT security regime. Even if complete coordination is not possible, the SC as a whole or a leading firm in the SC could set higher standards of IT security, which the incoming firm could emulate in equilibrium. This research emphasizes that collaboration in operational front alone may prove myopic unless integrated strategies are not appropriated in the changed IT security environment of the SC as a new firm comes on board. In essence, this observation suggests that firms in a SC should not be allowed to independently choose their IT security strategies, which proves to be the lowest order equilibrium among all the three decision scenarios.

Observation-4**:** *First mover strategy in an IT security game is costly; the leader has a higher IT security investment in comparison to that of the follower in the equilibrium*.

The opportunity of setting standards in terms of the sophistication and efficacy of IT security in a SC can be an important consideration for a leading firm in a SC. Although this increases the cost in the IT security regime for the leading firm, there are other advantages which may still justify this increased cost. For example, it may create an environment of higher trust and a higher level of appreciation of IT security in the incoming firm, which potentially benefits the SC over an extended horizon. One significant take away from this research is the following; - Since a supply chain may not be certain that an oncoming firm would be ready to decide their IT security issues under a common centralized coordination mechanism, it is a good idea to maintain a high standard of IT security and make it observable to any incoming firm, such that the resultant equilibrium IT security level of the SC remains better than the independent decision scenario.

Recollecting the Wal-Mart example from the introduction section in conjunction with the insight from observation-4, it appears that Wal-Mart does have a sound IT security strategy for the incoming firms: - By asking them to comply, Wal-Mart signals its leadership status in the IT security arena of the SC, and ensures at least the benefits of the higher level equilibrium of the leader-follower strategy that we have discussed in this section.

DISCUSSION AND CONCLUDING REMARKS

Utilizing a 2 firm simple supply chain we extend the research on interdependent IT security in general and IT security in supply chain in particular. Since firms in a supply chain share their information assets and networks to the other firms and employ transactional interconnectivity in order to enjoy symbiotic benefits, the IT security risk of the firms become interdependent in multiple dimensions. However, as practical observation suggests, cooperation in the operational front does not necessarily guarantee coordination in IT security initiatives, since this may involve sensitive informational contexts that the firms may not agree to share. As a result, there are multiple feasible decision scenarios in the overall IT security regime in a SC. We isolate 3 important decision scenarios from these possibilities and analyze the equilibrium investment and cost of IT security under each of these scenarios. We show that a centrally coordinated IT security regime works best in a SC - it has the lowest total cost of equilibrium IT security. On the other extreme, if the firms are unable to agree to a centralized decision scenario and take their independent decisions, they are worst of. The chain suffers from low IT security and costs dearly to the firms. However, if coordination is not possible, there is still a middle ground. In case there is a power structure in the SC, which is often the case in reality, a leading firm may set higher standards in IT security and then credibly signal that to the other firms. When the signal is credible and/or the high standards are observable, the follower firm/s invests at a level that the resultant cost of IT security of the SC falls somewhere between the two extreme decision scenarios.

This research is in an initial stage. The intractability of analytical solutions has been a major concern, and we are at work trying to simplify aspects of the models. Our future focus in this research is to conduct further analysis with the help of the exponential functional form that we have introduced here. We also propose to investigate the leader-follower game further under the incomplete information scenario. The managerial insights so far have been quite encouraging and we hope to enrich and extend these interesting findings in future.

REFERENCES

1. Bandyopadhyay, T., Jacob, V., Raghunathan, S. 2010. Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. Information Technology and Management, Volume 11, Number 1, 7-23.
2. Brousseau, E. 1994. EDI and Inter Firm Relationships: Toward a Standardization of Coordination Processes. Information, Economics and Policy, Vol. 6, 319-47.
3. Croom, S. R. 2000. The Impact of Web-based Procurement on the Management of Operating Resources Supply. Journal of Supply Chain Management. Winter 4-12.
4. Dearing, B. 1995. EDI: driving VAN growth. Telecommunications. June 69-73
5. Gal-Or, E., Ghose, A. 2005. The Economic Incentives for Sharing Security Information. Information Systems Research Vol. 16, No. 2, pp. 186–208.
6. Gordon Lawrence A., and Loeb Martin P. 2002. The Economics of Information Security Investment. ACM Transactions on Information and System Security. Vol. 5, No. 4, 438-457.
7. Gordon, Lawrence A., Loeb, P. Martin and Lucyshyn William. 2003. Sharing Information on Computer System Security. Journal of Accounting and Public Policy. Vol. 22.
8. Hagel III, J. and M. Singer. 1999. Unbundling the Corporation. Harvard Business Review. March/April 133-41.
9. Hausken, K. 2006. Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment. Journal of Accounting and Public Policy 25, 6, 629-665.
10. Hausken, K. 2007. Information Sharing among Firms and Cyber Attacks. Journal of Accounting and Public Policy 26, 6, 639-688.
11. Heal Geoffrey, and Kenreuther Howard. 2003. You Only Die Once: Managing Discrete Interdependent risk. National Bureau of Economic Research.
12. Kambil, A., P. F. Nunes and D. Wilson. 1999. Transforming the Market Space with All-in-one Markets. International Journal of Electronic Commerce. Vol. 3, 11-28.
13. Kaplan, S. and M. Sawhney. 2000. E-hubs: the New B2B Marketplaces. Harvard Business Review (May-June). 97-103.
14. Kekre, S. and Mukhopadhyay, T. 1992. Impact of Electronic Data Interchange Technology on Quality Improvement and Inventory Reduction Programs: a Field Study. International Journal of Production Economics. Vol. 28, 265-82.t Science, Vol. 40, No. 10, October (1994), 1291-1304.

15. Kunreuther, H., Heal, G., 2003. Interdependent security. The Journal of Risk and Uncertainty 26, 2/3, 231-249.
16. Niederman, F. 1998. The Diffusion of Electronic Data Interchange Technology. In Larsen, T. J. and E. McGuire (eds.) Information Systems Innovation and Diffusion: Issues and Directions. Idea Group Publishing, 141-60, Hershey.
17. Ogut H., Raghunathan, S., and Menon N. 2004. Self Protection and Insurance in IT security: the Case of Interdependencies. Working Paper, The University of Texas at Dallas.
18. Susarla, A., Barua, A., And Whinston, A. B. 2007. "An Empirical Analysis of Complementarity in Information Integration and Inter-Organizational Coordination". Working Paper, The University Of Texas At Austin
19. Srinivasan, K., S. Kekre, and T. Mukhopadhyay, Impact of Electronic Data Interchange Technology on JIT Shipments, Management Science, Vol. 40, No. 10, October (1994), 1291-1304.
20. Tanaka Hideyuki, Matsuura Kanta, and Sudoh Osamu. 2005. Vulnerability and Information Security Investment: an Empirical Analysis of E-local Government in Japan. Journal of Accounting and Public Policy. Vol. 24, No. 1, 37-59.
21. Varian Hal. 2002. System Reliability and Free Riding. Working Paper, The University of California at Berkeley.
22. Wang, E.T.G., and Seidman A. 1995. Electronic Data Interchange: Competitive Externalities and Strategic Implementation Policies. Management Science. Vol. 41, No. 3, 401-418.