2011

A Model for B2B IT Security: Multilayer Defense Facing Interdependent Cyber Risk

Tridib Bandyopadhyay
Kennesaw State University, tbandyop@kennesaw.edu

A Model for B2B IT Security: Multilayer Defense Facing Interdependent Cyber Risk

Tridib Bandyopadhyay
Kennesaw State University
tbandyop@kennesaw.edu

ABSTRACT

B2B firms couple their business processes for better efficiency. Integrated Business processes require that the firms' networks be interconnected. This practice enables breach incidence to travel from one firm to another, making the IT security risks of the firms strategically interdependent. The present practice of multilayered defense against IT breaches resembles stage-gates, bringing operational interdependency between the successive layers of defense in a B2B firm. Such inter-firm and inter-layer interdependences in B2B relationship ultimately results in complex decision scenarios in the IT security regime. We propose a comprehensive game theoretic model to capture the above complex, intertwined interdependencies of IT security risk in B2B firms. We also provide some initial results to explain the B2B firms' incentive to invest in IT security.

Keywords

IT Security, IT Security Investment, Game Theoretic Approach, B2B IT Security, Multilayer IT Security Defense

1. INTRODUCTION

Firms have been engaging in B2B relationships since quite some time now. Process integration, leading to gains in efficiency and increased cost effectiveness have remained the predominant driving forces. Of late, such motivation is further strengthened by the Internet technologies, which provide a cost effective networking option between B2B firms. Small and medium firms, which earlier found the costs of EDI networking technologies daunting, have now engaged in numerous B2B relationships with the help of the Internet based open standard technologies. Although inter-firm networking does bring business value, firms must also be aware of the cyber risks that can be propagated across the B2B firms with the help of these network interconnectivities. Since cyber risks are more likely to propagate over the open standard based Internet technologies than the proprietary EDI technologies, firms who engage in the Internet based B2B networking need to be especially careful about the interdependency in IT security risks that ensue. Importantly, this interdependency potentially impacts the motivation of the other interconnected firm to secure its own perimeter from the general web traffic. After all, if Firm-1 is not careful about its incoming web traffic, the trusted B2B connectivity that it maintains with Firm-2 is exposed to the rogue elements that may manage to filter through the porous perimeter security of firm-1. As a result, B2B firms' IT security initiatives become quite interdependent on each other (Bandyopadhyay et. al. 2010). While the strategic IT security interdependency remains a major concern for the B2B firms, there is yet another aspect of operational dependency that must be managed by a typical firm (including a B2B firm) in its IT security Domain.

Although researchers and practitioners have urged firms to manage their IT security risks in myriad ways (for a refresher, see Whitman et. al. 2010), one common theme that is widely accepted in IT security is the concept of 'defense in layers'. Firms today secure their network perimeters with the firewall technology to keep unwanted traffic out (prevention regime), yet implement Intrusion Detection Systems (IDS) in order to track and monitor filtered external traffic as well as the internal traffic (detection regime). Although effective, such layered approach is challenging in terms of the joint implementation, since the mutual configuration of the layers must ensure optimal balance between the needs of access control and information asset protection. The basic challenge arises from the fact that the layers of IT security defense somewhat resemble the sequenced stage-gates of a statistically controlled process. For example, if a firm employs a large cache of firewall rules, the firewall becomes very restrictive. As a result, the incidence rate on the IDS – the relative proportion of the rogue traffic in the filtered output from the firewall- sharply drops. This in turn, affects the statistical errors (the false positive and false negative ratios) of the IDS, thereby necessitating changes in the alarm investigation strategies of the defending firm! In other words, the configuration and the sensitivities of the layers of IT security defense are required to be in tune with one another in order to ensure an effective overall IT security defense. Proper mutual configuration cannot be overemphasized - under certain conditions; a firm with sub-optimally configured layered IT security defense may even do worse than the case where it employs only one of the IT security layers without the other (Cavusoglu et. al. 2009)!

The above sets of interdependencies, one from the strategic inter-firm B2B relationship and the other arising out of the need for operational configurations between the layers of technology in IT security, give rise to one challenging research question: *Given that (1) a typical firm must manage the operational interdependency between the layered IT security defenses, and that (2) the B2B firms experience strategic interdependency between their IT security risks,* ***How do the incentives of strategic IT security investment play out between the B2B firms***?

In this work, we attempt to seek answer to the above research question from a strategic view point. We propose a game theoretic model that comprehensively captures the interdependencies in IT security as faced by a modern B2B firm. The players in the proposed model are the defenders in IT security, namely the B2B firms. However, IT security defense must also be appropriately reactive to the Hackers, who are regarded as *strategic* in their actions. Thus, strategic hacking attacks are anticipated, and captured in our model in response to the relative IT security levels of the B2B firms. In order to keep the analytics tractable between the nested interdependencies of layered IT security defense within B2B relationship, we model a simple scenario where a unique hacker attacks one of the two symmetric B2B firms in the system. The contributions of this work are (a) we provide a game theoretic model for the layered IT security defense in B2B relationship and (b) we reconcile inter-firm strategic interdependencies and intra-firm operational interdependencies of layered IT security defense in a unique framework. To the best of our knowledge, neither of the above has been done before. Significantly, our work conjoins paradigms of IT security decisions that encompass multiple firms each securing its IT assets in a layered approach.

In what follows, we first provide a brief literature review in section-2 before we present our model and analyze some preliminary results of the model in section-3. We present our concluding thoughts and future research in section-4. This work is currently at an initial phase, and our emphasis in the paper have been on rationalizing the model scenario, capturing the risks of interdependency in B2B relationship and propose a model that abstracts realities of IT security defense in B2B yet retains analytical tractability and suggest managerial insights.

2. LITERATURE REVIEW

This work relates to the interdependence of IT security in firms and also to the theme of layered defense in IT security. We thus briefly provide reviews for the closely related literature in either of the above areas. Researchers in the economics of information systems literature have addressed investments in IT security. Gordon and Loeb (2002) have analyzed how vulnerabilities in IT security influence defending firms' investments. Their results have been later qualified and corroborated by Tanaka et. al.,(2005). Coming from the point of view that IT security in connected firms could be explained in the light of private provisioning of public goods, Varian (2002) has isolated the existence of free rider behavior in defending firms in the IT security arena. Kunreuther and Heal (2003) have also analyzed the interdependence between defending firms' IT security, and have further characterized firms' free rider behavior. Hausken (2006) has modeled the IT security investments as a resultant from the impacts of the defending firms' mutual interdependence, income, and substitution effects. Ogut et al. (2005) have differentiated IT security investments between technological and financial approaches and have shown general complementarities between these instruments. Bohme et. al. (2006) have shown that correlated cyber risks can create deficiencies in the supply side of financial instruments to manage cyber risks. Bandyopadhyay et. al. (2010) have modeled strategic decisions in the IT security defense of supply chain firms, who share information assets to mutual benefits. While Cavusoglu et. al. (2004) have analyzed the aspects of investments in IT security in the layers of Firewall and IDS technologies, Whitman et. al. (2010) have discussed the overall benefits of utilizing the layers of defense in IT security. In a late work, Cavusoglu et. al. (2009) have analyzed the interdependencies of configuration between the IDS and Firewall technologies and have noted the benefits of mutually optimal configurations between these technologies in layered IT security. In a sense, our present work brings the strategic framework and backgrounds from Bandyopadhyay et. al. (2010) and combines them with the intra-firm operational interdependencies of Cavusoglu (2009).

3. THE MODEL AND ANALYSIS

Our game theoretic model is set up in the backdrop of a B2B relationship between two Firms.

Each of the B2B firms, F_i, $i \in \{1,2\}$, has information asset which is the target of a hacker. In order to compromise an information asset, the hacker must penetrate the perimeter security of a firm who owns the information asset. Each firm employs firewall technology to keep unauthorized entry to its network to a minimum level. Other things remaining same, a higher investment (***x***) in firewall technology (***FW***) reduces the probability (***p***) that the hacker will be able to breach the perimeter security ($p'(x_i) < 0,\ p''(x_i) > 0$).

Each firm also employs ***IDS*** technology to monitor traffic inside its perimeter. If a hacker circumvents the perimeter security of a firm, it can be detected by the IDS technology with a success factor (***d***), which however depends on the commitment[1] (***y***) of the firm. Standard concavity assumptions in firm commitments on the IDS technologies apply ($d'(y_i) > 0, d''(y_i) < 0$).

The B2B firms share a dedicated interconnectivity. If the hacker gets inside the perimeter of a firm, it can then successively utilize this inter-firm connectivity to reach the other firm with a probability (***q***), whose magnitude depends on the utilized technology for inter-firm networking technology and is assumed independent of the detection of the hacking activity by the first firm.

A breach into a firm brings loss $L_i,\ i \in \{1,2\}$. Detection does not completely obviate loss but is assumed to attenuate the loss by a factor ($\alpha_i, 0 \le \alpha_i \le 1$), since such detection may occur after the hacker has been able to access the information asset. If a breach further propagates to the other firm through the interconnectivity, the originally breached firm suffers loss higher by a factor β_i, $(1 \le \beta_i)$ to account for the business embarrassment and other compensation requirements, if any.

The hacker's action (***H***) is implicitly strategic in the way it selects the target. By the processes of foot printing, fingerprinting and port scanning, the hacker is assumed to form an appreciation of the perimeter security of the firms, and targets that firm which has the lower level of perimeter security arrangements. The probability of an attack on firm 1 is denoted by $s = s(x_1, x_2), s'_{(x_1)} < 0, s'_{(x_2)} > 0$. For our 2-firm system, the probability of an attack on firm B is thus given by (*1*-*s*).

The contingency tree of the breach scenario in the B2B including the losses to the firms 1 and 2 is presented below.

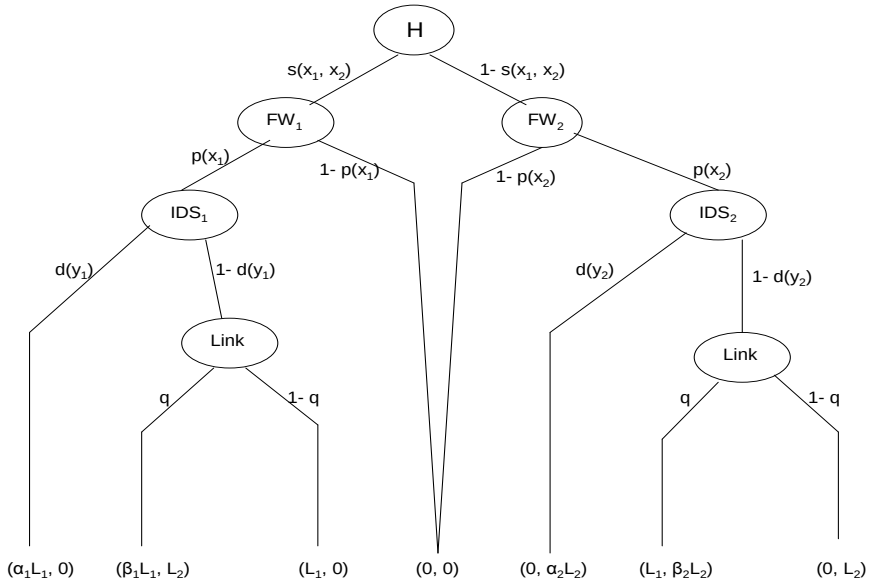

Figure-1 Scenario with attendant losses

3.1 The Model

The probability that Firm-1 enjoys freedom from any direct or indirect breach is given by[2] $(1-sp_1)(1-q(1-s)p_2)$. Thus the probability that there is at least a direct or indirect breach into Firm-1 is given by: $1-(1-sp_1)(1-q(1-s)p_2)$.

Consequently, the Expected loss to Firm-1 is given by: $\Psi_1 = [1-(1-sp_1)(1-q(1-s)p_2)][(1-d_1)\alpha_1 L_1 + (1-d_1)\beta_1 L_1]$

Finally, F-1 solves the following problem to optimally select its investments and commitments in the IT security defense:

[1] Such commitments come in the forms of managerial and technical investigation of alarms on top of the technological finding aspects including procurement, update and and management of IDS equipment, breach signatures, employee enablement and other authorization structures.

[2] For brevity, we write $p(x_1) = p_1$, $d(y_1) = d_1$ etc.

$$\Omega = \underset{x_1, y_1}{Min} \langle x_1 + y_1 + [1 - (1 - sp_1)(1 - q(1-s)p_2)][\beta_1(\alpha_1 L_1) + (1-d_1)\beta_1 L_1] \rangle \text{ or}$$
$$\Omega = \underset{x_1, y_1}{Min} \langle x_1 + y_1 + [p_1(1-qp_2) + qp_2(1-s+s^2 p_1)][\beta_1(\alpha_1 L_1) + (1-d_1)\beta_1 L_1] \rangle \quad \textbf{(1)}$$

3.2 Analysis of the Overall Breach Probabilities

Before we analyze the model, we investigate the overall breach probabilities of the firms. Since the probabilities of attack (*s*), probability of success in breaching the firewall (*p*), and the probability of cross-firm breach propagation (*q*) are each only a small fraction, we ensure simplicity of analysis by ignoring multiplicative terms involving 3 or more of these variables/parameters. As we exhibit in (*i*) through (*iii*), the movement of the breach probability with the investments in firewall and IDs technologies remain mixed across the firms, signifying complex interdependencies in IT security initiatives.

(*i*) $B[x_1, x_2] = 1 - (1 - sp_1)(1 - q(1-s)p_2)$,

Thus $\frac{\partial B_1}{\partial x_1} = s'_{(x_1)}[p_1(1-qp_2) + qp_2(2sp_1 - 1)] + p_1'[(1-qp_2) + s^2 qp_2] \approx s'_{(x_1)}[p_1 - qp_2] + p_1'[$

In other words, if p_1 and p_2 are comparable, and q is small, then $\frac{\partial B_1}{\partial x_1} < 0$. By similar treatment to the analog of (1), it is easy to see that $\frac{\partial B_2}{\partial x_2} < 0$ as well. However,

(*ii*) $\frac{\partial B_1}{\partial x_2} = s'_{(x_2)}[p_1(1-qp_2) + qp_2(2sp_1 - 1)] + p_2'[(1-s+s^2 p_1) - sp_1 q] \approx s'_{(x_2)}[p_1 - qp_2] + p_2'[(1-s)]$.

Clearly, even if p_1 and p_2 remain comparable, and q remains small as before, note that $\frac{\partial B_1}{\partial x_1} < 0$ is inconclusive since although $s'_{(x_2)} > 0$, $p_2' < 0$. Observation-1 is in order now:

<u>Observation-1</u>: Investment in its own firewall decreases overall breach probability of the same firm. However, the same insight does not extend to inter-firm impact of investments in firewall on the overall breach probabilities!

(*iii*) $\frac{\partial B_1}{\partial q} = -sp_1 p_2 + p_2(1-s+s^2 p_1) \approx p_2(1-s) \Rightarrow \frac{\partial B_1}{\partial q} > 0$, prompting the following observation:

<u>Observation-2</u>: The overall breach probability of either firm (similar analysis for firm-2 yields identical results) consistently increases in the inter-firm breach probability q.

3.3 Analysis of the Model

Now we proceed to the analysis of the Objective function (***OF***). First note that by our existing concavity assumptions and construction of the model, $s'_{(x_1)} < 0, s'_{(x_2)} > 0$; $p_1', p_2' < 0$, $d_1', d_2' > 0$. The first order conditions of the OF are:

$$p_1'(x_1^*) = \frac{-1}{\{s(1-qp_2) + qp_2 s^2\}}\left[\frac{1/L_1}{\{d_1\alpha_1 + (1-d_1)\beta_1\}} + s'_{(x_1^*)}[\beta_1(1-qp_2) + qp_2(2sp_1 - 1).]\right] \text{.....} \quad (2)$$

$$d_1'(y_1^*) = \left[\frac{-1/L_1}{(\alpha_1 - \beta_1)\{p_1(1-qp_2) + qp_2(1-s-s^2 p_1)\}}\right] \text{.....} \quad (3)$$

In order to garner meaningful insights yet keep the analytics simple, we impose symmetric conditions between the B2B firms, and investigate the simultaneous Nash equilibrium investments of the B2B firms:

$$p_1'(x_1^*) \approx \frac{-1/L_1}{s(1-qp_2)\{d_1\alpha_1 + (1-d_1)\beta_1\}} \text{ At symmerty.... } \Rightarrow \frac{-2/L}{(1-qp)\{\beta - d(\beta-\alpha)\}} \text{.....} \quad (4)$$

$$d_1'(y_1^*) \approx \frac{1/L_1}{(\beta_1-\alpha_1)\{sp_1 + qp_2\}} \text{ At symmerty... } \Rightarrow .. \frac{1/L}{(\beta-\alpha)\,p\,(s+q)} = \frac{1/L}{(\beta-\alpha)\,p\,\{s+2+q\}} \quad (5)$$

First note (4) and see that if the investment in IDS ***y*** goes up in equilibrium, the detection rate ***d*** increases, which in turn increases $\left|p_1'(x_1^*)\right|$. However, this is also tantamount to a decrease in investment in the firewall ***x*** in the equilibrium, since $p'(x) < 0.$ Now consider (5). If investment in firewall ***x*** goes up in equilibrium, then the probability of direct breach ***p*** falls and the magnitude of the acceleration in detection $\left|d_1'(y_1^*)\right|$ increases, which is equivalent to a decrease in the investment in the IDS (i.e., *y*) in the simultaneous Nash equilibrium. This leads to our Observation-3 below:

<u>Observation-3</u>: Investment in firewall and IDS technologies act as <u>strategic substitutes</u> for a firm in B2B relationship which employs layered defense strategy in IT security.

As we have already mentioned, one important characterization of the B2B scenario today is the deployment of open standard networking technologies to save cost while engaging in multiple relationships in a scalable and interoperable fashion. We have also alluded to the fact that these technologies are inherently less secure than the proprietary technologies like the EDI technology. As such these technologies are vendor specific and offer only some degree of security proofing. Consequently, it is important for us to investigate how the IT security health of the interconnecting technology affects the motivation of investment of the B2B firms in firewall and IDS technologies.

Since we allow both the investments in firewall and IDS to vary simultaneously on the vulnerability of the interconnecting technology, we first present the Hessian conditions of the objective function Ω before we present the full differentials of the layered investments of the B2B firms. Note that we have omitted the mathematical derivations for paucity of space, and have presented only the final expressions below.

While the hessian conditions are:

$$i)\ \frac{\partial^2\Omega}{\partial x^2} > 0, \quad ii)\ \frac{\partial^2\Omega}{\partial y^2} > 0, iii) - sp''(AML)d''(LEB) - \{(sp'd')(ABL)^2\} > 0, \quad or, \quad sp''d''(ME) + (AB)(sp'd')^2 < 0$$

The solution for the full differentials yield:

$$\left\langle \frac{dx}{dq} = \frac{spp'\{d''(ME) - d'^2(ABC)\}}{A\{p''d''(ME) + (AB)(sp'd')^2\}}\frac{dy}{dq} = \frac{spMd'\{(p')^2 - p''C\}}{\{p''d''(ME) + (AB)(sp'd')^2\}} \right\rangle$$

$$Where \quad M_1 = [d_1\alpha_1 + (1-d_1)\beta_1], \quad A = (1-qp_2), \quad B = (\beta_1 - \alpha_1), \quad C = (1-s-sp_1) \quad E = \{sp_1 + qp_2(1-s-sp_1)\};$$

Note that the denominator of the differentials is negative (vide the Hessian conditions).

Observations-4 and 5 are in order now:

<u>Observation-4</u>: Facing increased vulnerability in the interconnecting technology, a B2B firm's equilibrium investment in firewall decreases in presence of IDS technology as an integral part of its layered defense strategy in IT security.

The above observation is disturbing. It is easy to see that an increased vulnerability in networking technology increases breach probability **B (x_1, x_2)** and if this now prompts a decrease in the equilibrium investment in firewall technology in presence of IDS, the B2B firm's IT security posture stands to suffers seriously!

Observation-5**: Facing increased vulnerability in the interconnecting technology, a B2B firm's equilibrium investment in IDS decreases when* $\frac{(p')^2}{p''} > \frac{1-s-sp}{s}$ ***, else its investment in IDS technology increases in presence of firewall technology.

4. CONCLUDING REMARKS:

Beginning with a simple 2-firm contingency tree of IT security breach, we have developed a game theoretic model to examine how firms in a B2B relationship, who face network vulnerability in terms of cross propagation of breach incidence from one firm to another, may react in terms of their investments in the layered IT defense strategies. The relationships thus explored suggest deep complexity and interdependence in IT risk between the B2B firms, which we have presented in the numerous observations in the analysis section. We have attempted to capture two recent phenomena of B2B landscape, namely the widespread business process integration especially in the SME segment, and the current trend to implement cost effective B2B networking solutions which operate on the Internet. Since the benefits are compelling and the vendors promote their B2B networking solutions aggressively, these cost effective technologies exhibit great patronage. Our analysis shows that these B2B firms need to be careful when they decide on such products, services and relationships. Understanding and reacting to the strategic IT risks of B2B relationship, especially when the firms also employ layered IT defense strategy, appears to be a challenging task. Our model is a modest attempt to help such understanding processes towards better management of IT security risk in B2B relationship. This research is in an initial stage of development. Our model is well thought out, and the primary analysis of the model appears promising. Our future goal is analyze the complex risks and investment strategies in a threadbare fashion, and provide complete analysis of the model. Although we have analyzed simultaneous investment strategies of the firms here, the analysis can also be extended for sequential or Stackelberg type games, which are appropriate for B2B relationships that exhibit leader-follower structures or Hub-and-spoke topologies. Our work can also be extended for cases, where the leadership structure in a B2B relationship may shoulder the responsibility to implement and manage a centrally optimized multilayer IT defense regime.

References

1. Bandyopadhyay, T., Raghunathan, S, Jacob, V. 2010. Information Security in Networked Supply Chains: Impact of Network Vulnerability and Supply Chain Integration on Incentives to Invest. Information Technology and Management. 11(1). 7-23.
2. Bohme, R., Kataria, G. 2006. Models and Measures for Correlation in Cyber Insurance. In the Proceedings of the Workshop on the Economics of Information Security. Boston, USA.
3. Cavusoglu, H., Mishra, B., Raghunathan, S. 2004. A Model for Evaluating IT Security Investments. Communications of the ACM. 47(7). 87-92.
4. Cavusoglu, H., Raghunathan, S., Cavusoglu, H. 2009. Configuration of and Interaction between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. Information Systems research. 20(2). 198-217.
5. Gordon L. A., and Loeb M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*. Vol. 5, No. 4, 438-457.
6. Gordon, L. A., Loeb, P. M., and Lucyshyn W. 2003. Sharing Information on Computer System Security. Journal of Accounting and Public Policy. Vol. 22.
7. Hausken, K. (2006). Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment. *Journal of Accounting and Public Policy* 25, 6, 629-665.
8. Kunreuther, H., Heal, G., 2003. Interdependent security. *The Journal of Risk and Uncertainty* 26, 2/3, 231-249.
9. Tanaka H,, Matsuura K., and Sudoh O. (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.
10. Varian Hal. (2002). System Reliability and Free Riding. Working Paper. The University of California at Berkeley.
11. Whitman, M., Mattord, H. 2010. Management of Information Security, Third edition. Cengage Publications, USA.