A Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints

Anna Nagurney
Isenberg School of Management
University of Massachusetts, Amherst, Massachusetts 01003
Patrizia Daniele
Department of Mathematics and Computer Science
University of Catania, Italy
and
Shivani Shukla
Isenberg School of Management
University of Massachusetts, Amherst, Massachusetts 01003

February 2015; revised November 2015
Annals of Operations Research (2017), **248(1)**, pp. 405-427.

Abstract: In this paper, we develop a supply chain network game theory model consisting of retailers and demand markets with retailers competing noncooperatively in order to maximize their expected profits by determining their optimal product transactions as well as cybersecurity investments subject to nonlinear budget constraints that include the cybersecurity investment cost functions. The consumers at the demand markets reflect their preferences through the demand price functions, which depend on the product demands and on the average level of cybersecurity in the supply chain network. We identify the supply chain network vulnerability to cyberattacks as well as that of the individual retailers. We demonstrate that the governing Nash equilibrium conditions can be formulated as a variational inequality problem and we provide a novel alternative formulation, along with the accompanying theory. We also propose an algorithm for the alternative formulation, which yields, at each iteration, closed form expressions in product transactions, security levels, and Lagrange multipliers associated with the budget constraints. We then apply the algorithm to compute solutions to a spectrum of numerical supply chain network cybersecurity investment examples. The examples broaden our understanding of the impacts of the addition of retailers, changes in budgets, demand price functions, and financial damages, on equilibrium product transactions and cybersecurity investments, as well as on the supply chain network vulnerability and retailer vulnerability under budget constraints.

Key words: cybersecurity, investments, game theory, Nash equilibrium, information asymmetry, variational inequalities, supply chain network vulnerability

1. Introduction

The challenges imposed by the growing number of cyberattacks, along with the associated financial losses and reputational costs, are testing businesses and other organizations, governments, and even individuals. Recent and highly visible cyberattacks have included the cyberbreach at the financial services giant JPMorgan in late summer 2014, which affected 76 million customers (Caruthers (2014), Glazer (2015)), the security breach at the retail giant Target in late 2013 with an estimated 40 million payment cards stolen and upwards of 70 million other personal records compromised (Kirk (2014)), and the data breach at SONY Pictures in late Fall 2014, which has been called catastrophic and a public relations nightmare (Lewis (2014)). According to PricewaterhouseCoopers (2014a), the number of cybersecurity incidents that were detected by respondents to their survey increased by 48% to 42.8 million in 2014. At the same time, the number that reported losses of $20 million or greater was almost double the number reported in 2013. No industrial sector is immune to cyberattacks with sectors such as financial services, healthcare, high technology, energy, and governments being especially attractive targets (see Nagurney (2015)). Also, as noted therein, the Center for Strategic and International Studies (2014) reports that the estimated annual cost to the global economy from cybercrime is more than $400 billion with a conservative estimate being $375 billion in losses, a number that exceeds the national income of most countries.

In today's networked economy, many businesses are dependent on their globalized supply chains with their IT infrastructure increasingly spread out and, at the same time, vulnerable to cyberattacks. For example, the Target breach of 2013 occurred when the cyberattacker took advantage of the vulnerability in the remote diagnostics of the HVAC system supplier connected to Target's IT system and entered a vulnerable supply chain link (Nagurney, Nagurney, and Shukla (2015)). Hence, there is a growing interest in developing rigorous frameworks for cybersecurity investments. According to PricewaterhouseCoopers (2014a), mid-sized and large companies reported a 5% increase in cybersecurity budgets, whereas small companies reduced security costs by more than 20%. As reported in Glazer (2015), JPMorgan is expected to double its cybersecurity spending in 2015 to $500 million from $250 million in 2015. According to Purnell (2015), the research firm Gartner reported in January 2015 that the global information security spending would increase by 7.6% this year to $790 billion and by 36% by 2018 to $101 billion. It is clear that making the best cybersecurity investments, given budget constraints, is a very timely problem and issue.

Whether in retail, financial services, government settings, energy, healthcare, or others, it is essential to recognize that the cybersecurity investments of one member of a supply

chain in terms of cybersecurity may impact the probability of a successful cyberattack on another. The IT infrastructure may be shared; suppliers may be common; the members may have similar vulnerabilties, and so on. Hence, to truly capture the impacts of cybersecurity investments, one needs to model not only the individual cybersecurity investment problem but that of multiple decision-makers simultaneously. Therefore, a game theory framework is needed.

In this paper, we develop a supply chain network game theory model of cybersecurity investments consisting of a tier of retailers and a tier of demand markets. The retailers can be consumer goods retailers, high tech retailers, or even financial service ones. What is needed is that they are in the same industry and that their individual decisions may impact the decisions of the others in terms of the volume of product handled and the level of cybersecurity investment. Our work builds on that of Shetty (2010), Shetty et al. (2009), and Nagurney, Nagurney, and Shukla (2015) but with a crucial difference – the retailers are now subject to individual budget constraints for their cybersecurity investments. These constraints are nonlinear, posing challenges for both theory and computations. In addition, unlike in Nagurney, Nagurney, and Shukla (2015), in our new game theory model we allow each retailer to have a distinct upper bound on its security level, which is less than one, with a value of one corresponding to perfect security, which may not be achievable. In our earlier work, all retailers had an upper bound of one on their security levels. In addition, in the new model in this paper, we also impose upper bounds on the product transactions between retailers and the consumers at the demand markets. For a survey of game theory, as applied to network security and privacy, see Manshaei et al. (2013). Rue, Pfleeger, and Ortiz (2007), on the other hand, provide an overview of models for cybersecurity investments, ranging from input/output models to return on investment frameworks as well as heuristic approaches. The edited volume by Daras and Rassias (2015) contains a collection of papers on cryptography and network security.

Our contributions to the literature lie in advancing the state-of-the-art of game theory for cybersecurity investments as well as applications of variational inequalities, with the accompanying theory, for problems with nonlinear constraints. To-date, with the exception of the work of Toyasaki, Daniele, and Wakolbinger (2014), in the realm of network equilibrium models for end-of-life products, there has been limited work on such problems.

We now highlight the importance of having models for cybersecurity investments that include budget constraints. Specifically, we further emphasize the economic and cyberattack landscape today. Cybersecurity has become an innate part of every organization's IT infrastructure. Most operational and policy related decisions include cybersecurity implica-

tions. From a system standpoint, organizations have to deploy a lot more than firewalls. Defense against risks originating from both within and outside the organization needs significant investments to keep up with the threats. Unfortunately, budget constraints can delay implementation of security measures and in the event of a successful cyberattack cause heavy losses. Even though companies are investing more than they used to in cybersecurity, mounting risks caused 65% respondents in a survey to state that budget constraints are their number one obstacles to delivering value (EY (2013)). Moreover, most of the budget gets spent on resolving past issues rather than investing in future protection. According to a report on cybercrime in the U.S. by PricewaterhouseCoopers (2014b), Retailers spend $400 per employee while banks and other financial service institutions spend as much as $2500 on cybersecurity. An increase in budget could lower the risk; however, it would not make companies immune to cyberattacks. To strategically use a constrained budget is the best option.

For instance, Sony Pictures plans to spend $15 million to secure itself from future cyberattacks. The company had been attacked in 2014 that costed it $100 million (IT Security (2015)). With a tight budget set aside, protecting employees and infrastructure, and monitoring interactions with other competitors and partners would be a challenge. Despite a budget of $250 million, JP Morgan Chase was attacked in 2014 since they neglected investing into two-step authentication. Target after its attack in 2014 that cost $148 million assigned a budget of $100 million that was used specifically to adopt a technology to embed chips into debit and credit cards for added security (CBS News (2014)). Having committed a chunk of funds for technology, investment in other cybersecurity measures would certainly be constrained. Earlier cybersecurity investments were considered pure costs that do not add to the brand or the products. However, with the sheer volume of attacks and vulnerabilities within the organization to patch, IT needs have grown. If large companies are facing a budget constraint, small companies are facing a decline in cybersecurity spending, making them a perfect target for infiltration (Statista (2015)).

This paper is organized as follows. In Section 2, we develop the supply chain network game theory model with competing retailers, who seek to individually maximize their expected utilities, which capture the expected revenue and financial losses, in the case of a cyberattack, along with the costs associated with cybersecurity investments. We also discuss how to measure the vulnerability of a firm to cyberattacks and that of the supply chain network, as a whole. We state the Nash equilibrium conditions, present the theoretical foundations, and provide variational inequality formulations. In the first variational inequality formulation, the nonlinear budget constraints appear in the feasible set and, in the alter-

native one, through the use of Lagrange multipliers, the nonlinear constraints are captured in the function that enters the variational inequality with the feasible set consisting of the nonnegative orthant and the bounds on the security levels. In Section 3, we present the algorithm, with nice features for computations, that yields, at each iteration, closed form expressions for the product transactions, the security levels, and the Lagrange multipliers associated with the budget constraints of the retailers. In Section 4, we present the numerical examples and, in Section 5, we summarize and conclude.

2. The Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints

The supply chain network game theory model of cybersecurity investments with nonlinear budget constraints consists of m retailers, with a typical retailer denoted by i, and n demand markets, with a typical demand market denoted by j. Retailers may be brick and mortar stores or online retailers. In our framework, we consider *retailer* in a broad sense in that a retailer may correspond to a financial service firm such as a retail bank, a consumer goods store, etc. We do assume that the retailers transact the same product. Since we are concerned with cybersecurity investments, the transactions between the two tiers take place electronically in terms of payments and, hence, there may be a possibility of cyberattacks with the concomitant financial damage, loss of reputation, opportunity costs, and associated disruptions. Specifically, consumers at the demand markets make their purchases by credit or debit cards or via an online payment system. They reflect their preferences as to the cybersecurity of the supply chain network through the demand price functions. The information that they have available is the average supply chain network cybersecurity, which we refer to as the supply chain network security or, simply, the network security. We can expect consumers at the demand markets to have information as to the security in an industry rather than the individual retailer cybersecurity levels. Since here we are concerned with supply chain aspects, the retailers share some connectivity and may be exposed to cyberattacks through their suppliers, and/or possibly, common payment systems, or even computer infrastructure.

The bipartite network structure of the problem is depicted in Figure 1 and the notation for the model is presented in Table 1.

We first present the constraints and then we construct the objective function of each retailer. We also discuss how we quantify the cybersecurity of the supply chain network along with its vulnerability, and that of the individual retailers. One of the challenging aspects of the model is that the budget constraints are nonlinear and, hence, convexity of

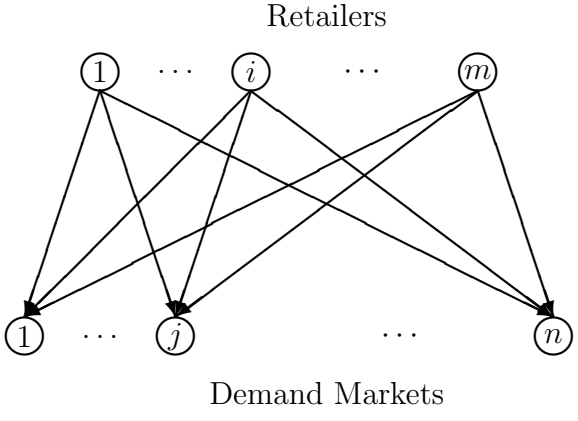

Figure 1: The Bipartite Structure of the Supply Chain Network Game Theory Model

Table 1: Notation for the Model

Notation	**Definition**
Q_{ij}	the amount of the product transacted between retailer i and demand market j; $i = 1, \ldots, m$; $j = 1, \ldots, n$. We group the transactions $\{Q_{ij}\}$ for retailer i into the vector $Q_i \in R^n_+$ and all the transactions of all retailers into the vector $Q \in R^{mn}_+$.
d_j	the demand for the product at demand market j; $j = 1, \ldots, n$. We group the demands into the vector $d \in R^n_+$.
s_i	the cybersecurity level of retailer i; $i = 1, \ldots, m$. We group the security levels of all retailers into the vector $s \in R^m_+$.
$\bar{s}$	the cybersecurity level in the supply chain network, where $\bar{s} = \frac{1}{m}\sum_{k=1}^{m} s_k$.
p_i	the probability of a successful cyberattack on retailer i
c_i	the cost associated with handling and processing the product at retailer i; $i = 1, \ldots, m$.
$c_{ij}(Q_{ij})$	the transaction cost associated with transacting between i and j; $i = 1, \ldots, m$; $j = 1, \ldots, n$.
$\rho_j(d, \bar{s})$	the demand price of the product at demand market j; $j = 1, \ldots, n$.
B_i	the budget of retailer i for cyberinvestments, which cannot be exceeded; $i = 1, \ldots, m$.
D_i	the financial damage accrued by retailer i after a successful cyberattack on i; $i = 1, \ldots, m$.
$\bar{Q}_{ij}$	the upper bound on the product transaction between i and j; $i = 1, \ldots, m$; $j = 1, \ldots, n$.
u_{s_i}	the upper bound on the security level of retailer i; $i = 1, \ldots, m$.

the feasible sets of the retailers must be established.

The demand for the product at demand market j must satisfy the following conservation

of flow equation:

$$d_j = \sum_{i=1}^{m} Q_{ij}, \quad j = 1, \ldots, n, \tag{1}$$

where

$$0 \leq Q_{ij} \leq \bar{Q}_{ij}, \quad i = 1, \ldots, m; j = 1, \ldots, n, \tag{2}$$

that is, the demand at each demand market is satisfied by the sum of the product transactions between all the retailers with the demand market, and these transactions must be nonnegative and not exceed the imposed upper bounds.

The cybersecurity level or, simply, security, of each retailer i must satisfy the following constraint:

$$0 \leq s_i \leq u_{s_i}, \quad i = 1, \ldots, m, \tag{3}$$

where $u_{s_i} < 1$ for all i; $i = 1, \ldots, m$. The larger the value of s_i, the higher the security level, with perfect security reflected in a value of 1, but, since we do not expect perfect security to be attainable, we have $u_{s_i} < 1$; $i = 1, \ldots, m$. If $s_i = 0$ this means that retailer i has no security.

Associated with acquiring a security level s_i is an investment cost function h_i; $i = 1, \ldots, m$, with the function assumed to be continuously differentiable and convex. We assume that, for a given retailer i, $h_i(0) = 0$ denotes an entirely insecure retailer and $h_i(1) = \infty$ is the investment cost associated with complete security for the retailer. An example of an $h_i(s_i)$ function satisfies these properties and that we utilize in our model as

$$h_i(s_i) = \alpha_i\left(\frac{1}{\sqrt{(1 - s_i)}} - 1\right) \text{ with } \alpha_i > 0. \tag{4}$$

The term α_i enables distinct retailers to have different investment cost functions based on their size and needs. Such functions have been introduced by Shetty (2010) and Shetty et al. (2009) and also used by Nagurney, Nagurney, and Shukla (2015). However, in those models, there are no cybersecurity budget constraints and the cybersecurity investment cost functions only appear in the objective functions of the decision-makers.

In our model, each retailer is faced with a limited budget for cybersecurity investment. Hence, the following nonlinear budget constraints must be satisfied:

$$\alpha_i\left(\frac{1}{\sqrt{(1 - s_i)}} - 1\right) \leq B_i; \quad i = 1, \ldots, m, \tag{5}$$

that is, each retailer can't exceed his allocated cybersecurity budget. Clearly, the constraints in (5) are nonlinear and pose challenges for the analysis and solution of our model, which we demonstrate can be overcome.

As in Shetty et al. (2009) and Shetty (2010), we define the probability p_i of a successful cyberattack on retailer i as

$$p_i = (1 - s_i)(1 - \bar{s}), \quad i = 1, \ldots, m, \tag{6}$$

where the term $(1-\bar{s})$ represents the probability of a cyberattack on the supply chain network and the term $(1 - s_i)$ represents the probability of success of such an attack on retailer i. The supply chain network vulnerability level $\bar{v} = 1 - \bar{s}$ with retailer i's vulnerability level v_i being $1 - s_i$; $i = 1, \ldots, m$. Such measures are also used in Nagurney, Nagurney, and Shukla (2015).

In view of (1) we can define demand price functions $\hat{\rho}_j(Q, s) \equiv \rho_j(d, \bar{s}), \forall j$. The consumers reflect their preferences for the product through the demand price functions, which depend not only on the vector of demands but also on the supply chain network security. We expect the consumers to be willing to pay more for enhanced network security but the degree may differ from consumer to consumer. Also, there is information asymmetry (cf. Akerlof (1970)) in the model, since retailers are aware of their investments in cybersecurity, but consumers know only the average security as defined by $\bar{s}$.

The profit f_i of retailer i; $i = 1, \ldots, m$ (in the absence of a cyberattack and security investment) is the difference between the revenue and his costs, that is,

$$f_i(Q, s) = \sum_{j=1}^{n} \hat{\rho}_j(Q, s) Q_{ij} - c_i \sum_{j=1}^{n} Q_{ij} - \sum_{j=1}^{n} c_{ij}(Q_{ij}). \tag{7}$$

If there is a successful cyberattack on a retailer i; $i = 1, \ldots, m$, he incurs an expected financial damage given by

$$D_i p_i, \tag{8}$$

where D_i takes on a positive value.

Using expressions (6), (7), and (8), the expected utility, $E(U_i)$, of retailer i; $i = 1, \ldots, m$, which corresponds to his expected profit, is:

$$\begin{aligned} E(U_i) &= (1 - p_i) f_i(Q, s) + p_i(f_i(Q, s) - D_i) - h_i(s_i)) \\ &= f_i(Q, s) - p_i D_i - h_i(s_i). \end{aligned} \tag{9}$$

According to (9), each retailer encumbers the cost associated with his cybersecurity investment. We group the expected utilities of all the retailers into the m-dimensional vector $E(U)$ with components: $\{E(U_1), \ldots, E(U_m)\}$.

Let K^i denote the feasible set corresponding to retailer i, where $K^i \equiv \{(Q_i, s_i) | 0 \leq Q_{ij} \leq \bar{Q}_{ij}, \forall j, , \text{ and } 0 \leq s_i \leq u_{s_i} \text{ and } (5) \text{ holds for } i\}$ and define $K \equiv \prod_{i=1}^{m} K^i$.

The m retailers compete noncooperatively in supplying the product and invest in cybersecurity, each one trying to maximize his own expected profit. We seek to determine a nonnegative product transaction and security level pattern $(Q^*, s^*) \in K$ for which the m retailers will be in a state of equilibrium as defined below. Nash (1950, 1951) generalized Cournot's concept (see Cournot (1838)) of an equilibrium for a model of several players, that is, decision-makers, each of which acts in his/her own self-interest, in what has been come to be called a noncooperative game.

Definition 1: A Supply Chain Nash Equilibrium in Product Transactions and Security Levels

A product transaction and security level pattern $(Q^*, s^*) \in K$ is said to constitute a supply chain Nash equilibrium if for each retailer $i; i = 1, \ldots, m$,

$$E(U_i(Q_i^*, s_i^*, \hat{Q}_i^*, \hat{s}_i^*)) \geq E(U_i(Q_i, s_i, \hat{Q}_i^*, \hat{s}_i^*)), \quad \forall (Q_i, s_i) \in K^i, \tag{10}$$

where

$$\hat{Q}_i^* \equiv (Q_1^*, \ldots, Q_{i-1}^*, Q_{i+1}^*, \ldots, Q_m^*); \quad \textit{and} \quad \hat{s_i^*} \equiv (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_m^*). \tag{11}$$

According to (10), a supply chain network equilibrium is established if no retailer can unilaterally improve upon his expected profits by selecting an alternative vector of product transactions and security levels.

We now present alternative variational inequality formulations of the above supply chain Nash equilibrium in product transactions and security levels.

We first establish that the feasible set K is convex in the following lemma. In our model, unlike in many network equilibrium problems from congested urban transportation networks to supply chains and financial networks (cf. Nagurney (1999, 2006), Daniele (2006)), the feasible set contains nonlinear constraints.

Lemma 1

Let h_i be a convex function for all retailers i; $i = 1, \ldots, m$. The feasible set K is then convex.

Proof: We study the convexity of the constraint set

$$\bar{K} = \{s_i \in R : h_i(s_i) \leq B_i\}. \tag{12}$$

Let s_i^1, $s_i^2 \in \bar{K}$ and $\lambda \in [0, 1]$, namely:

$$h_i(s_i^1) \leq B_i \text{ and } h_i(s_i^2) \leq B_i. \tag{13}$$

Since $h_i(s_i)$ is a convex function, we have:

$$h_i\left(\lambda s_i^1 + (1-\lambda)s_i^2\right) \leq \lambda \underbrace{h_i(s_i^1)}_{\leq B_i} + (1-\lambda)\underbrace{h(s_i^2)}_{\leq B_i} \leq B_i, \tag{14}$$

namely,

$$h_i\left(\lambda s_i^1 + (1-\lambda)s_i^2\right) \leq B_i, \tag{15}$$

that is,

$$\lambda s_i^1 + (1-\lambda)s_i^2 \in \bar{K}. \tag{16}$$

Hence, the set defined by (12) is convex.

Also, we know that each K_i consists of the above budget constraint, the box-type constraint (3) on s_i, and the nonnegativity constraints on retailer i's transactions as in (2). The intersection of these sets is also convex. Finally, since K is the Cartesian product of convex sets, K_i; $i = 1, \ldots, m$, it is also convex, so the conclusion follows. □

We note that each investment cost function $h_i(s_i)$; $i = 1, \ldots$, as in (4), and defined on $[0, u_{s_i}]$ is convex since its second derivative is positive. Indeed,

$$h_i'(s_i) = \frac{\alpha_i}{2}(1 - s_i)^{-\frac{3}{2}} \quad \text{and} \quad h_i''(s_i) = \frac{3\alpha_i}{4}(1 - s_i)^{-\frac{5}{2}} > 0. \tag{17}$$

Theorem 1: Variational Inequality Formulation

Assume that, for each retailer i; $i = 1, \ldots, m$, the expected profit function $E(U_i(Q, s))$ is concave with respect to the variables $\{Q_{i1}, \ldots, Q_{in}\}$, and s_i, and is continuously differentiable. Then $(Q^*, s^*) \in K$ is a supply chain Nash equilibrium according to Definition 1 if and only if it satisfies the variational inequality

$$-\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} \times (Q_{ij} - Q_{ij}^*) - \sum_{i=1}^{m} \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0, \quad \forall (Q, s) \in K, \tag{18}$$

or, equivalently, $(Q^*, s^*) \in K$ is a supply chain Nash equilibrium product transaction and security level pattern if and only if it satisfies the variational inequality

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\left[c_i + \frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} \times Q_{ik}^*\right] \times (Q_{ij} - Q_{ij}^*)$$

$$+\sum_{i=1}^{m}\left[\frac{\partial h_i(s_i^*)}{\partial s_i} - (1 - \sum_{k=1}^{m}\frac{s_k^*}{m} + \frac{1 - s_i^*}{m})D_i - \sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q_{ik}^*\right] \times (s_i - s_i^*) \geq 0,$$

$$\forall (Q, s) \in K. \tag{19}$$

Proof: From Lemma 1 we know that the feasible set for each retailer i, K_i; $i = 1, \ldots, m$, is convex as is the Cartesian product of these sets, K. Under the imposed assumptions on the expected utility functions of the retailers, according to Proposition 2.2 in Gabay and Moulin (1980), which established the equivalence between the solution to a Nash equilibrium problem and the solution to the corresponding variational inequality problem, we know that each retailer i; $i = 1, \ldots, m$, maximizes his expected utility according to Definition 1 if and only if

$$-\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} \times (Q_{ij} - Q_{ij}^*) - \sum_{i=1}^{m}\frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0, \quad \forall s_i \in [0, u_{s_i}], \tag{20}$$

which is precisely variational inequality (18).

In order to obtain variational inequality (19) from variational inequality (18), we note that, at the equilibrium:

$$-\frac{\partial E(U_i)}{\partial Q_{ij}} = c_i + \frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} \times Q_{ik}^*; \quad i = 1, \ldots, m; j = 1, \ldots, n; \tag{21}$$

and

$$-\frac{\partial E(U_i)}{\partial s_i} = \frac{\partial h_i(s_i^*)}{\partial s_i} - (1 - \sum_{k=1}^{m}\frac{s_k^*}{m} + \frac{1 - s_i^*}{m})D_i - \sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q_{ik}^*; \quad i = 1, \ldots, m. \tag{22}$$

Substituting the above expressions into variational inequality (20), we obtain variational inequality (18). □

We now put variational inequality (18) into standard variational inequality form, that is: determine $X^* \in \mathcal{K} \subset R^N$, such that

$$\langle F(X^*), X - X^* \rangle \geq 0, \quad \forall X \in \mathcal{K}, \tag{23}$$

where F is a given continuous function from $\mathcal{K}$ to R^N and $\mathcal{K}$ is a closed and convex set.

We define the $(mn + m)$-dimensional column vector $X \equiv (Q, s)$ and the $(mn + m)$-dimensional column vector $F(X) \equiv (F^1(X), F^2(X))$ with the (i, j)-th component, F^1_{ij}, of $F^1(X)$ given by

$$F^1_{ij}(X) \equiv -\frac{\partial E(U_i(Q, s))}{\partial Q_{ij}}, \tag{24}$$

the i-th component, F^2_i, of $F^2(X)$ given by

$$F^2_i(X) \equiv -\frac{\partial E(U_i(Q, s))}{\partial s_i}, \tag{25}$$

and with the feasible set $\mathcal{K} \equiv K$. Then, clearly, variational inequality (18) can be put into standard form (23).

In a similar way, one can prove that variational inequality (19) can also be put into standard form (23).

Additional background on the variational inequality problem can be found in the book by Nagurney (1999).

Remark

If the retailers are not subject to budget constraints, $u_{s_i} = 1$, for $i = 1, \ldots, m$, and there are no upper bounds on the product transactions, then the above model collapses to the model in Nagurney, Nagurney, and Shukla (2015) with the associated variational inequalities having the same structure as those in (18) and (19) but with a substantially simpler feasible set which consists of the nonnegative orthant for the product transactions and the security levels, with the latter also bounded from above by one. Such a model, nevertheless, can be used to identify the (Q^*, s^*) under "ideal" unlimited conditions as to budgets and product transactions.

We now provide some qualitative properties, in terms of existence and uniqueness of a solution to variational inequality (18).

Theorem 2: Existence

A solution (Q^*, s^*) to variational inequality (18) (equivalently, (19)) is guaranteed to exist.

Proof: The result follows from the classical theory of variational inequaliities (see Kinderlehrer and Stampacchia (1980)) since the feasible set K is compact, and the function that enters the variational inequality (cf. (23) – (25)) is continuous. □

Moreover, we also have the following result.

Theorem 3: Uniqueness

The solution (Q^*, s^*) to variational inequality (18) is unique if the function $F(X)$ as in (23), with components defined by (24) and (25), and $X \equiv (Q, s)$ is strictly monotone, that is:

$$\langle (F(X^1) - F(X^2)), X^1 - X^2 \rangle > 0, \quad \forall X^1, X^2 \in \mathcal{K}, \quad X^1 \neq X^2. \tag{26}$$

Proof: See Kinderlehrer and Stampacchia (1980).

We know that the function $F(X)$ is strictly monotone over $\mathcal{K}$ if its Jacobian $\nabla F(X)$ is positive definite over $\mathcal{K}$.

Since the feasible set K has nonlinear constraints and this may pose challenges for numerical computations, we now derive an alternative variational inequality to (19) which incorporates Lagrange multipliers. Specifically, we associate the Lagrange multiplier $\lambda_i \geq 0$; $i = 1, \ldots, m$, with the budget constraint (5), respectively, for each retailer $i = 1, \ldots, m$. We group these Lagrange multipliers into the vector $\lambda \in R^m_+$. The new variational inequality is defined over the feasible set $\mathcal{K}^2 \equiv \prod_{i=1}^m \mathcal{K}^1_i \times R^m_+$, where $\mathcal{K}^1_i \equiv \{(Q_i, s_i) | Q_i \geq 0; 0 \leq s_i \leq u_{s_i}\}$.

We show in Section 3 that this novel variational ienquality will be amenable to solution via an iterative scheme that is straightforward to implement.

Theorem 4: Alternative Variational Inequality Formulation

A vector $(Q^*, s^*, \lambda^*) \in \mathcal{K}^2$ is a solution to variational inequality (19) if and only if it is a solution to the variational inequality:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \left[c_i + \frac{\partial c_{ij}(Q^*_{ij})}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} \times Q^*_{ik} \right] \times (Q_{ij} - Q^*_{ij})$$

$$+ \sum_{i=1}^{m} \left[\frac{\partial h_i(s^*_i)}{\partial s_i} - (1 - \sum_{k=1}^{m} \frac{s^*_k}{m} + \frac{1 - s^*_i}{m}) D_i - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q^*_{ik} + \frac{\lambda^*_i}{2} \alpha_i (1 - s^*_i)^{-\frac{3}{2}} \right] \times (s_i - s^*_i)$$

$$+ \sum_{i=1}^{m} \left[B_i - \alpha_i (\frac{1}{\sqrt{(1 - s^*_i)}} - 1) \right] \times (\lambda_i - \lambda^*_i)) \geq 0, \quad \forall (Q, s, \lambda) \in \mathcal{K}^2. \tag{27}$$

Proof: Each retailer i; $i = 1, \ldots, m$, according to Definition 1, seeks to determine his strategy vector (Q_i, s_i) so as to

$$\text{Maximize}_{(Q_i, s_i)} \; E(U_i) = (1 - p_i) f_i(Q, s) + p_i(f_i(Q, s) - D_i) - h_i(s_i) \tag{28}$$

subject to:

$$\alpha_i(\frac{1}{\sqrt{(1 - s_i)}} - 1) - B_i \leq 0,$$
$$0 \leq Q_{ij} \leq \bar{Q}_{ij}, \quad j = 1, \ldots, n,$$
$$0 \leq s_i \leq u_{s_i},$$

where $f_i(Q, s)$ is given by (7), $h_i(s_i)$ is given by (4), and $p_i = (1 - s_i)(1 - \bar{s})$.

Simplifying the terms in the objective function (28) and converting the Maximization problem into a Minimization problem, the above optimization problem with the newly defined feasible set $\mathcal{K}_i^1$ becomes:

$$\text{Minimize} \quad - f_i(Q, s) + D_i(1 - s_i)(1 - \bar{s}) + h_i(s_i) \tag{29}$$

subject to:

$$\alpha_i(\frac{1}{\sqrt{(1 - s_i)}} - 1) - B_i \leq 0,$$
$$(Q_i, s_i) \in \mathcal{K}_i^1.$$

If we now let $X_i \equiv (Q_i, s_i)$, $\hat{X}_i \equiv (X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_m)$, and $\hat{f}_i(X_i, \hat{X}_i) \equiv -f_i(Q, s) + D_i(1 - s_i)(1 - \bar{s}) + h_i(s_i)$, we can rewrite retailer i's optimization problem, where $\hat{X}_i^*$ denotes the other retailers' optimal solutions, as:

$$\text{Minimize} \quad \hat{f}_i(X_i, \hat{X}_i^*) \tag{30}$$

subject to:

$$g_i(X_i) \leq 0, \tag{31}$$
$$X_i \in \mathcal{K}_i^1. \tag{32}$$

Note that $g_i(X_i) = \alpha_i(\frac{1}{\sqrt{(1 - s_i)}} - 1) - B_i$.

We now form the Lagrangian $\mathcal{L}(X_i, \hat{X}_i^*, \lambda_i) = \hat{f}_i(X_i, \hat{X}_i^*) + \lambda_i g_i(X_i)$.

Also, we make the following assumption:

Assumption: (Slater Condition). There exists a Slater vector $\tilde{X}_i \in \mathcal{K}_i^1$ for each $i = 1, \ldots, m$, such that $g_i(\tilde{X}_i) < 0$.

This is easy to verify.

Then, according to Koshal, Nedic, and Shanbhag (2011), pages 1049-1051, since $\hat{f}_i$ is convex in X_i and is continuously differentiable and g_i is also convex and continuously differentiable, and $\mathcal{K}_i^1$ is nonempty, closed and convex, $(X_i^*, \lambda_i^*) \in \mathcal{K}_i^1 \times R_+$ is a solution to the above optimization problem (30), subject to (31) and (32), if and only if it is a solution to the variational inequality:

$$\nabla_{X_i} \mathcal{L}(X_i^*, \hat{X}_i^*, \lambda_i^*) \times (X_i - X_i^*) + (-g_i(X_i^*)) \times (\lambda_i - \lambda_i^*) \geq 0, \quad \forall (X_i, \lambda_i) \in \mathcal{K}_i^1 \times R_+, \quad (33)$$

with $\nabla_{X_i} \mathcal{L}$ representing the gradient with respect to X_i of the Lagrangian $\mathcal{L}$.

Expanding (33) by using the definitions of our functions and vectors and making the appropriate substitutions, we obtain that $X_i^* \in \mathcal{K}_i^1$ is a solution to (33) if and only if $(Q_i^*, s_i^*, \lambda_i^*) \in \mathcal{K}_i^1$ is a solution to the variational inequality:

$$\sum_{j=1}^{n} \left[c_i + \frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} \times Q_{ik}^* \right] \times (Q_{ij} - Q_{ij}^*)$$

$$+ \left[\frac{\partial h_i(s_i^*)}{\partial s_i} - (1 - \sum_{k=1}^{m} \frac{s_k^*}{m} + \frac{1 - s_i^*}{m}) D_i - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q_{ik}^* + \frac{\lambda_i^*}{2} \alpha_i (1 - s_i^*)^{-\frac{3}{2}} \right] \times (s_i - s_i^*)$$

$$+ \left[B_i - \alpha_i (\frac{1}{\sqrt{(1 - s_i^*)}} - 1) \right] \times (\lambda_i - \lambda_i^*) \geq 0, \quad \forall (Q_i, s_i, \lambda_i) \in \mathcal{K}_i^1. \quad (34)$$

But inequality (34) holds for each i; $i = 1, \ldots, m$, since we are dealing with a Nash equilibrium problem, so summation of (34) over all i; $i = 1, \ldots, m$, we obtain variational inequality (27). $\square$

We now put variational inequality (27) into standard form (23). Let $X \equiv (Q, s, \lambda)$ and let $F(X) \equiv (\hat{F}^1(X), \hat{F}^2(X), \hat{F}^3(X))$ be the $(mn + 2m)$-dimensional vector consisting of components: $\hat{F}_{ij}^1(X)$; $i = 1, \ldots .m$; $j = 1, \ldots, n$, $\hat{F}_i^2(X)$; $i = 1, \ldots, m$, and $\hat{F}_i^3(X)$; $i = 1, \ldots, m$, where:

$$\hat{F}_{ij}^1(X) \equiv \left[c_i + \frac{\partial c_{ij}(Q_{ij})}{\partial Q_{ij}} - \hat{\rho}_j(Q, s) - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q, s)}{\partial Q_{ij}} \times Q_{ik} \right], \forall i, \forall j,$$

$$\hat{F}_i^2(X) \equiv \left[\frac{\partial h_i(s_i)}{\partial s_i} - (1 - \sum_{j=1}^{m} \frac{s_j}{m} + \frac{1 - s_i}{m}) D_i - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q, s)}{\partial s_i} \times Q_{ik} + \frac{\lambda_i}{2} \alpha_i (1 - s_i)^{-\frac{3}{2}} \right], \quad \forall i,$$

$$\hat{F}_i^3(X) \equiv \left[B_i - \alpha_i (\frac{1}{\sqrt{(1 - s_i)}} - 1) \right], \forall i.$$

Also, let $\mathcal{K} \equiv \mathcal{K}^2$. Then, clearly, variational inequality (27) can be put into standard form (23).

3. The Computational Procedure

The variational inequality (27) is amenable to solution via the Euler method of Dupuis and Nagurney (1993), which, at each iteration yields closed form expressions for the production transactions, the security levels, and the Lagrange multipliers.

Specifically, iteration τ of the Euler method where the variational inequality is expressed in standard form (26) is given by:

$$X^{\tau+1} = P_{\mathcal{K}}(X^{\tau} - a_{\tau}F(X^{\tau})), \tag{35}$$

where $P_{\mathcal{K}}$ is the projection on the feasible set $\mathcal{K}$ and F is the function that enters the variational inequality problem (23), where recall that $X \equiv (Q, s, \lambda)$ and $F(X)$ now consists of the components as defined following (34).

As established in Dupuis and Nagurney (1993), for convergence of the general iterative scheme, which induces the Euler method, the sequence $\{a_{\tau}\}$ must satisfy: $\sum_{\tau=0}^{\infty} a_{\tau} = \infty$, $a_{\tau} > 0$, $a_{\tau} \rightarrow 0$, as $\tau \rightarrow \infty$. Conditions for convergence for a variety of network-based problems can be found in Nagurney and Zhang (1996) and Nagurney (2006).

Explicit Formulae for the Euler Method Applied to the Game Theory Model

The elegance of this algorithm for our variational inequality (27) for the computation of solutions to our model is apparent from the following explicit formulae. In particular, we have the following closed form expression for the product transactions $i = 1, \ldots, m; j = 1, \ldots, n$:

$$Q_{ij}^{\tau+1} = \max\{0, \min\{\bar{Q}_{ij}, Q_{ij}^{\tau} + a_{\tau}(\hat{\rho}_j(Q^{\tau}, s^{\tau}) + \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^{\tau}, s^{\tau})}{\partial Q_{ij}} Q_{ik}^{\tau} - c_i - \frac{\partial c_{ij}(Q_{ij}^{\tau})}{\partial Q_{ij}})\}\}, \tag{36}$$

the following closed form expressions for the security levels, and for the Lagrange multipliers, respectively, for $i = 1, \ldots, m$:

$$s_i^{\tau+1} =$$

$$\max\{0, \min\{u_{s_i}, s_i^{\tau} + a_{\tau}(\sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^{\tau}, s^{\tau})}{\partial s_i} Q_{ik}^{\tau} - \frac{\partial h_i(s_i^{\tau})}{\partial s_i^{\tau}} + (1 - \sum_{j=1}^{m} \frac{s_j^{\tau}}{m} + \frac{1 - s_i}{m}) D_i) - \frac{\lambda_i^{\tau}}{2} \alpha_i (1 - s_i^{\tau})^{-\frac{3}{2}}\}\}. \tag{37}$$

$$\lambda_i^{\tau+1} = \max\{0, \lambda_i^{\tau} + a_{\tau}(-B_i + \alpha_i(\frac{1}{\sqrt{1 - s_i^{\tau}}} - 1))\}. \tag{38}$$

4. Numerical Examples

We implemented the Euler method, as discussed in Section 3, using FORTRAN on a Linux system at the University of Massachusetts Amherst. The convergence criterion was

$\epsilon = 10^{-4}$. The Euler method was considered to have converged if, at a given iteration, the absolute value of the difference of each product transaction and each security level differed from its respective value at the preceding iteration by no more than ϵ.

The sequence $\{a_\tau\}$ was: $.1(1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3} \ldots)$. We initialized the Euler method by setting each product transaction $Q_{ij} = 1.00, \forall i, j$, the security level of each retailer $s_i = 0.00, \forall i$, and the Lagrange multiplier for each retailer's budget constraint $\lambda_i = 0.00; \forall i$. The capacities $\bar{Q}_{ij}$ were set to 100 for all i, j.

The examples were constructed to reflect recent data in specific industrial reports as discussed below.

The examples had transaction cost functions of the following form:

$$c_{ij}(Q_{ij}) = a_{ij}Q_{ij}^2 + b_{ij}Q_{ij}, \quad i = 1, \ldots, m; j = 1, \ldots, n$$

and demand price functions of the following form:

$$\hat{\rho}_j(Q, s) = -m_j(\sum_{i=1}^{m} Q_{ij}) + r_j(\sum_{i=1}^{m} \frac{s_i}{m}) + q_j. \quad j = 1, \ldots, n$$

with a_{ij}, b_{ij}, m_j, r_j, and q_j all greater than zero, for all i and j.

Note that the transaction cost functions are strictly convex and the demand price functions are decreasing in the quantity demanded at a demand market but increasing in the average security level at the demand market. We expect that the consumers are willing to pay a higher price for a higher level of average security. The transaction cost functions include the transportation costs and having such functions being increasing functions of the product volume has been used in many network equilibrium problems (see Nagurney (1999, 2006) and the references therein).

It is straightforward to verify that, with the above functions, the assumptions of Theorem 1 hole. Indeed, we have that for all i and j:

$$\frac{\partial^2 E(U_i)}{\partial Q_{ij}^2} = -2m_{ij} - 2a_{ij} < 0$$

and

$$\frac{\partial^2 E(U_i)}{\partial s_i^2} = -\frac{3\alpha_i}{4}(1 - s_i)^{-\frac{5}{3}} - 2\frac{D_i}{m} < 0, \quad \forall s_i \in [0, u_{s_i}].$$

Hence, the expected utility of each retailer i, $E(U_i)$; $i = 1, \ldots, m$, is concave with respect to its strategic variables: Q_{i1}, Q_{i2}, ..., Q_{in}, and s_i. In fact, these functions are strictly concave. Clearly, the expected utilities are also twice continuously differentiable.

4.1 Examples 1 and 2 with Sensitivity Analysis

Examples 1 and 2, with the accompanying sensitivity analysis, consist of two retailers and two demand markets as depicted in Figure 2.

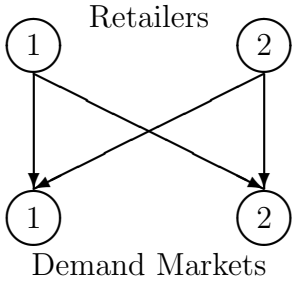

Figure 2: Network Topology for Examples 1 and 2 and Sensitivity Analysis

Example 1 and Sensitivity Analysis

The cost function data for Example 1 are:

$$c_1 = 5, \quad c_2 = 10,$$

$$c_{11}(Q_{11}) = .5Q_{11}^2 + Q_{11}, \quad c_{12}(Q_{12}) = .25Q_{12}^2 + Q_{12},$$
$$c_{21}(Q_{21}) = .5Q_{21}^2 + 2, \quad c_{22}(Q_{22}) = .25Q_{22}^2 + Q_{22}.$$

The demand price functions are:

$$\rho_1(d, \bar{s}) = -d_1 + .1(\frac{s_1 + s_2}{2}) + 100, \quad \rho_2(d, \bar{s}) = -.5d_2 + .2(\frac{s_1 + s_2}{2}) + 200.$$

The damage parameters are: $D_1 = 50$ and $D_2 = 70$ with the investment functions taking the form:

$$h_1(s_1) = \frac{1}{\sqrt{(1 - s_1)}} - 1, \quad h_2(s_2) = \frac{1}{\sqrt{(1 - s_2)}} - 1.$$

The damage parameters are in millions of \$US, the expected profits (and revenues) and the costs are also in millions of \$US. The prices are in thousands of dollars and the product transactions are in thousands. The budgets for the two retailers are identical with $B_1 = B_2 = 2.5$ (in millions of \$US). These data are representative for financial damages, due to a cyberattack, as reported by Yakowicz (2014), and for cybersecurity budgets of medium-sized to large firms, as reported by PricewaterhouseCoopers (2014a) in their survey.

The computed equilibrium solution for this example is given in Table 2. We know that this equilibrium solution is unique for the product transactions and the security levels since the

Table 2: Equilibrium Solution for Example 1

Solution	Example 1
Q_{11}^*	24.27
Q_{12}^*	98.34
Q_{21}^*	21.27
Q_{22}^*	93.34
d_1^*	45.55
d_2^*	191.68
s_1^*	.91
s_2^*	.91
$\bar{s}^*$	.91
λ_1^*	0.00
λ_2^*	0.00
$\rho_1(d_1^*, \bar{s}^*)$	54.55
$\rho_2(d_2^*, \bar{s}^*)$	104.34
$E(U_1)$	8137.38
$E(U_2)$	7213.49

Jacobian of the $F(X)$ that enters variational inequality (23) is strictly diagonally dominant and, hence, positive definite.

Retailer 1 has .21 (in millions) in unspent cybersecurity funds whereas Retailer 2 has .10 (in millions) in unspent funds. Hence, the associated Lagrange multipliers $\lambda_1^* = \lambda_2^* = 0.00$.

Both retailers have a firm vulnerability of .09 and the network vulnerability is, hence, also .09.

We then proceeded to conduct the following sensitivity analysis. We kept the budget of Retailer 2 fixed at 2.5 (in millions of \$US dollars), and we varied the budget of Retailer 1 from $B_1 = 1$ to $B_1 = 2.5$ in increments of .5. The values for the equilibrium security levels of the retailers, along with the network vulnerability, are reported in Figure 3. Figure 3 shows that, as the budget of Retailer 1 increases, its equilibrium security level increases, and the network vulnerability decreases. Hence, even Retailer 2 benefits from an increase in budget of Retailer 1.

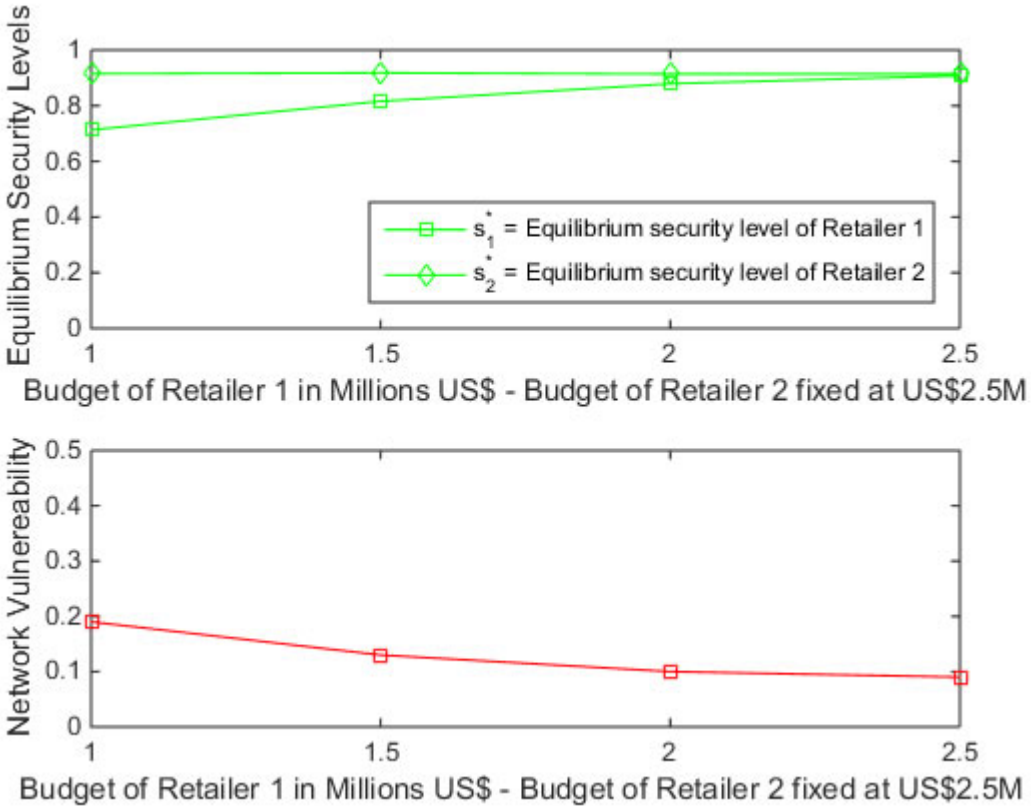

Figure 3: Sensitivity Analysis for Example 1 for Budget Size Variations of Retailer 1 with Retailer 2's Budget Fixed

Example 2 and Sensitivity Analysis

Example 2 was constructed from Example 1 and had the same data except that the investment cost function for Retailer 1 is now changed to:

$$h_1(s_1) = 10\frac{1}{\sqrt{(1-s_1)}} - 1.$$

Such a change in an investment cost function could occur, for example, in the case of acquisition of additional computers that need to be protected with additional associated costs. The equilibrium solution is reported in Table 2. We also checked for the uniqueness of the equilibrium product transaction and security level pattern examining the Jacobian $\nabla F(X)$ with F(X) as in (23) for this example which is strictly diagonally dominant.

Table 3: Equilibrium Solution for Example 2

Solution	Example 2
Q_{11}^*	24.27
Q_{12}^*	98.31
Q_{21}^*	21.27
Q_{22}^*	93.31
d_1^*	45.53
d_2^*	191.62
s_1^*	.36
s_2^*	.91
$\bar{s}^*$	.63
λ_1^*	3.68
λ_2^*	1.06
$\rho_1(d_1^*, \bar{s}^*)$	54.53
$\rho_2(d_2^*, \bar{s}^*)$	104.32
$E(U_1)$	8122.77
$E(U_2)$	7207.47

With higher security investment cost for Retailer 1, in Example 2, he invests less in security then he had in Example 1. The average security drops from $\bar{s}^* = .91$ in Example 1 to $\bar{s}^* = .63$ in Example 2 so that the network vulnerability $\bar{s} = .09$ in Example 1 whereas $\bar{v} = .37$ in Example 2, an increase of over a factor of 4. Also, the equilibrium Lagrange multipliers are now no longer equal to 0.00 since the budgets of both retailers are now fully spent. The equilibrium product flows remain the same or decrease slightly. Both firms suffer a drop in expected profits.

We then proceeded to conduct a similar sensitivity analysis as was conducted for Example

1. The results are reported in Figure 4. The network vulnerability is consistently higher for each datapoint in Figure 4 as compared to the respective datapoint in Figure 3.

These results demonstrate how increased cybersecurity investment costs can dramatically affect the vulnerability of the supply chain network as to cyberattacks. Also, they reveal that the budget size of one retailer can have system-wide effects not only in terms of network vulnerability but also in terms of expected profits.

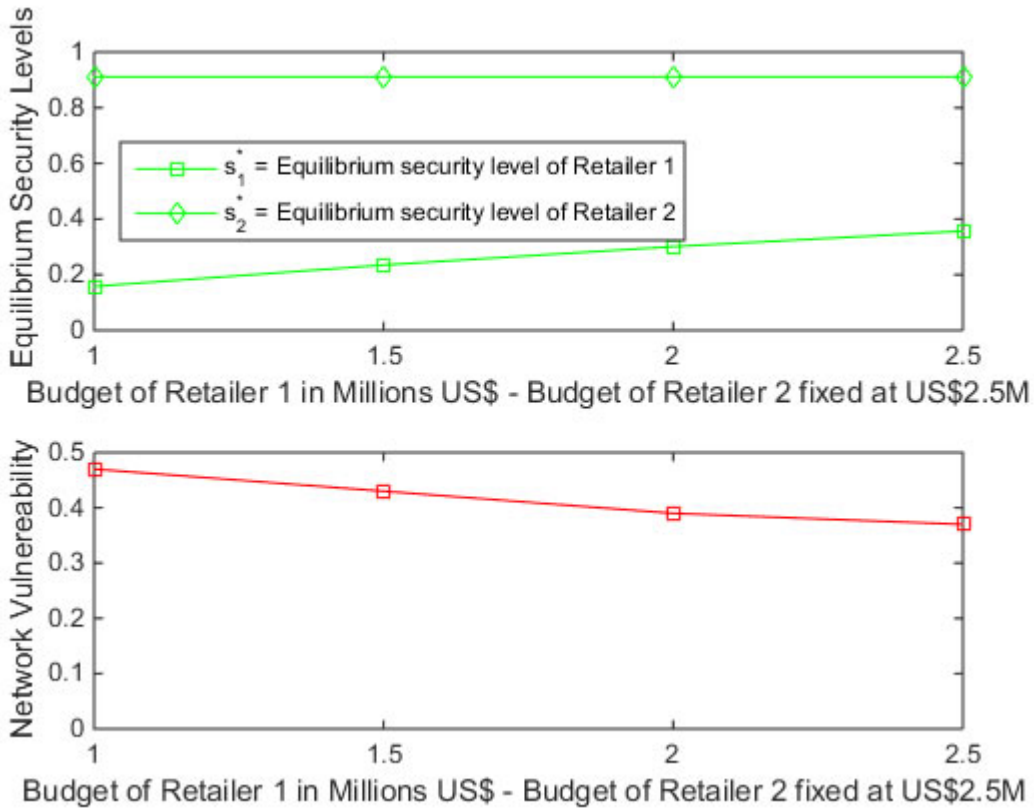

Figure 4: Sensitivity Analysis for Example 2 for Budget Size Variations of Retailer 1 with Retailer 2's Budget Fixed

4.2 Examples 3 and 4 with Sensitivity Analysis

Examples 3 and 4 consist of 3 retailers and 2 demand markets as depicted in Figure 5.

Example 3 and Sensitivity Analysis

Example 3 is constructed from Example 1 except for the new Retailer 3 data as given below:

$$c_3 = 3, \quad c_{31}(Q_{21}) = Q_{21}^2 + 3Q_{21}, \quad c_{32}(Q_{32}) = Q_{22}^2 + 4Q_{22},$$

$$h_3(s_3) = 3(\frac{1}{\sqrt{(1-s_3)}} - 1), \quad D_3 = 80.$$

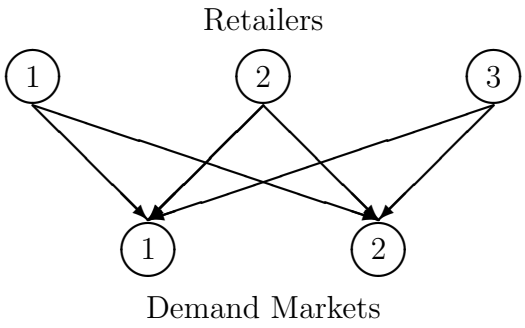

Figure 5: Network Topology for Examples 3 and 4 with Sensitivity Analysis

The budget for Retailer 3 is 3.0 (in millions of $US).

The equilibrium solutions for Example 3 are reported in Table 4.

Table 4: Equilibrium Solution for Example 3

Solution	Example 3
Q_{11}^*	20.80
Q_{12}^*	89.48
Q_{21}^*	17.80
Q_{22}^*	84.48
Q_{31}^*	13.87
Q_{32}^*	35.40
d_1^*	52.48
d_2^*	209.36
s_1^*	.90
s_2^*	.91
s_3^*	.74
λ_1^*	0.00
λ_2^*	0.00
λ_3^*	0.00
$\bar{s}^*$	.85
$\rho_1(d_1^*, \bar{s}^*)$	47.61
$\rho_2(d_2^*, \bar{s}^*)$	95.49
$E(U_1)$	6655.13
$E(U_2)$	5828.82
$E(U_3)$	2262.26

With the addition of Retailer 3, there is now increased competition. As a consequence, the demand prices for the product drop at both demand markets and there is an increase in demand. Also, with the increased competition, the expected profits drop for the two original

retailers. The demand increases for Demand Market 1 and also for Demand Market 2, both at upwards of 10%.

The vulnerability of Retailer 1 is .10, that of Retailer 2: .09, and that of Retailer 3: .26 with a network vulnerability of: .15. The network vulnerability, with the addition of Retailer 3 is now higher, since Retailer 3 does not invest much in security due to the higher investment cost.

Interestingly, all retailers do not exhaust their cybersecurity budgets. This may be due, in part, to information asymmetry in that the consumers at the demand markets only know the average security in the network and, hence, a retailer may invest less in cybersecurity. Hence, Retailer 3 is, in a sense, a "free rider."

We conduct the following sensitivity analysis. The coefficient in the demand price function at Demand Market 1 is .1. We proceed to increase this coefficient to 1.0, 2.0, and 3.0, and report the percent increase in expected profits of the retailers in Figure 6. All retailers benefit financially from consumers' higher valuation placed on average network security. These examples demonstrate that consumer awareness to supply chain network security, even in an average sense, can benefit retailers in terms of expected profits.

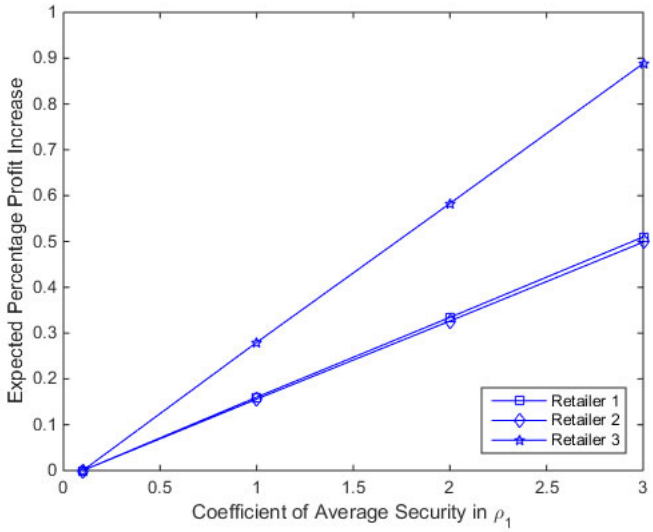

Figure 6: Sensitivity Analysis for Example 3 for Changes in ρ_1 Average Security Level Coefficient

Example 4 and Sensitivity Analysis

Example 4 is constructed from Example 3 as follows. The data are identical except that all the damages: $D_1 = D_2 = D_3 = 0.00$. The computed equilibrium solution is given in Table

5.

Table 5: Equilibrium Solution for Example 4

Solution	Example 4
Q_{11}^*	20.80
Q_{12}^*	89.43
Q_{21}^*	17.80
Q_{22}^*	84.47
Q_{31}^*	13.87
Q_{32}^*	35.40
d_1^*	52.47
d_2^*	209.30
s_1^*	.82
s_2^*	.81
s_3^*	.34
λ_1^*	0.00
λ_2^*	0.00
λ_3^*	0.00
$\bar{s}^*$	.66
$\rho_1(d_1^*, \bar{s}^*)$	47.60
$\rho_2(d_2^*, \bar{s}^*)$	95.48
$E(U_1)$	6652.45
$E(U_2)$	5828.10
$E(U_3)$	2264.24

Increased competition from Retailer 3 continues to increase the demand and decrease the prices when compared to Examples 1 and 2. However, with a sharp decrease in the damage parameters, that is, from $D_1 = 50, D_2 = 70, D_3 = 80$ to $D_1 = D_2 = D_3 = 0.00$, we observe a fall in the security levels for all the retailers. The average network security is down to 0.66 from 0.85 in the previous example. The vulnerability of Retailer 1 is 0.18, that of Retailer 2 is 0.19, and that of Retailer 3 is 0.66. Retailer 3, having a high investment cost, seems is the most vulnerable due to low investments in cybersecurity.

Interestingly, all retailers do not exhaust their cybersecurity budgets. This may be due, in part, to information asymmetry in that the consumers at the demand markets only know the average security in the network and, hence, a retailer may invest less in cybersecurity.

In Figure 7 we display the results of the following sensitivity analysis. We increase the damages for the retailers from $D_1 = D_2 = D_3 = 0.00$ to $D_1 = D_2 = D_3 = 5.00$ and then to $D_1 = D_2 = D_3 = 10.00$, followed by increments of 10.00 through 30.00. As

the damages increase, the average security levels go up and the network vulnerability goes down. Retailers become more sensitive to building security as the damages accrued due to a successful cyberattack increase.

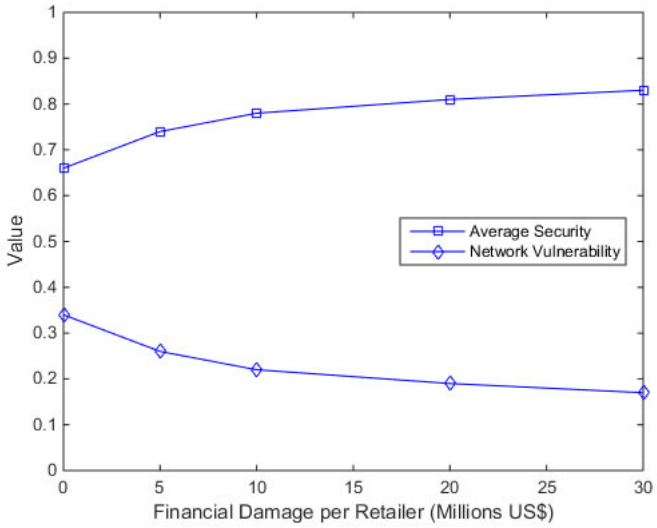

Figure 7: Sensitivity Analysis for Example 4 for Changes in Financial Damages with $D_1 = D_2 = D_3$

5. Summary, Conclusions, and Suggestions for Future Research

Increasing cybercrime incidents, and associated impacts, emphasize the importance of investment into counteracting these events for companies and other organizations, including financial institutions, retailers, and governments. Several of the recent notable data breaches and thefts have been reported by retailers in the United States, wherein financial damage, theft of critical information, and reputation loss took place. Complexities in the supply chains with numerous spatially dispersed entry points have led to loopholes that attackers have exploited. Retailers, being in the forefront, have become highly susceptible to breaches and ensuing losses. As a result, they seek to determine the optimal level of investments to be made given strict budget constraints for cybersecurity. This paper builds a general framework for quantifying these investments in the backdrop of competing retailers trying to maximize their expected profits subject to budget constraints. The game theory framework also identifies the vulnerability of the individual retailers and that of the supply chain network on the whole.

We develop a bipartite supply chain network game theory model consisting of retailers and demand markets. The retailers may be subject to a cyberattack and seek to maximize their expected profits by selecting their optimal product transactions and cybersecurity levels.

The retailers compete noncooperatively until a Nash equilibrium is achieved, whereby no retailer can improve upon his expected profit. The probability of a successful attack on a retailer, in our framework, depends not only on his security level, but also on that of the other retailers. Consumers at the demand markets reveal their preferences for the product through the demand price functions, which depend on the demand and on the network security level, which is the average security of the supply chain network. We include nonlinear investment cost functions levied on each retailer which is bounded by a budget level. These nonlinear budget constraints are incorporated into a variational inequality formulation through two alternative variational inequality formulations.

The governing equilibrium conditions and convexity of the feasible set have been derived for the variational inequalities, and the solvability is demonstrated with an appropriate algorithm with features supporting computations. Specifically, the algorithm yielded closed form expressions for the product transactions between retailers and demand markets, the security levels of retailers, as well as the Lagrange multipliers associated with the budget constraints at each iteration. Various data instances are evaluated through the algorithm, with relevant managerial insights and sensitivity analysis. The latter is conducted on the budgets, the coefficients of the demand price functions, and the damage parameters for pertinent analysis. The examples illustrate the impacts of an increase in competition, changes in the demand price functions, changes in the damages incurred, and changes in the cybersecurity investment cost functions, and budgets on the equilibrium solutions and on the incurred prices and the expected profits of the retailers. We also provide the vulnerability of each retailer in each example and the network vulnerability.

The generalized framework of cybersecurity investments in a supply chain network game theory context with nonlinear budget constraints is a novel contribution to the literature of both variational inequalities and game theory, and cybersecurity investments. The results in this paper pave the way for a range of investigative questions and research avenues in this area. For instance, at present, the model considers retailers and consumers in the supply chain network. However, it can be extended to include additional tiers, namely, suppliers, as well as transport service providers, and so on. Also, a case study and empirical analysis can further strengthen the validity of the model and assist in the process of arriving at investment decisions related to cybersecurity for specific companies/organizations. We leave the above research directions for future work.

Acknowledgments

This research of the first author was supported by the National Science Foundation (NSF) grant CISE #1111276, for the NeTS: Large: Collaborative Research: Network Innovation Through Choice project awarded to the University of Massachusetts Amherst as well as by the Advanced Cyber Security Center through the grant: Cybersecurity Risk Analysis for Enterprise Security. This support is gratefully acknowledged.

The authors thank the two anonymous reviewers for their careful reading of the original manuscript and many constructive comments, which have improved the presentation of the results.

References

Akerlof, G.A. (1970). The market for lemons: Quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, 84(3), 488-500.

Caruthers, R. (2014). JPMorgan will double cybersecurity spending but many other companies may cut costs. *Fierce Financial IT*, October 14.

CBS News (2014). Why $250 million didn't protect JP Morgan from hackers. Retrieved from: http://www.cbsnews.com/news/why-250m-didnt-protect-jp-morgan-from-hackers/

Center for Strategic and International Studies (2014). Net losses: Estimating the global cost of cybercrime. Santa Clara, California.

Cournot, A. A. (1838). *Researches into the mathematical principles of the theory of wealth*, English translation. London, England: MacMillan.

Daniele, P. (2006). *Dynamic networks and evolutionary variational inequalities*. Cheltenham, England: Edward Elgar Publishing.

Daras, N.J., & Rassias, M.T. (Eds.) (2015). *Computation, cryptography, and network security*. Switzerland: Springer International Publishing.

Dupuis, P., & Nagurney, A. (1993). Dynamical systems and variational inequalities. *Annals of Operations Research*, 44, 9-42.

EY (2013). Under cyber attack: EYs global information security report. Retrieved from: http://www.ey.com/Publication/vwLUAssets/EY-2013
_Global_Information - _Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf

Gabay, D., & Moulin, H. (1980). On the uniqueness and stability of Nash equilibria in noncooperatiive games. In A. Bensoussan, P. Kleindorfer, and C. S. Tapiero (Eds.), *Applied stochastic control in econometrics and management science* (pp. 271-294). Amsterdam, The Netherlands: North-Holland.

Glazer, E (2015). J.P. Morgan to accelerate timeline for cybersecurity spending boost. *The Wall Street Journal*, August 3.

IT Security (2015). Sony spends $15 million on security industry views. Retrieved from: http://www.itsecurityguru.org/2015/02/04/sony-spends-15-million-security-industry-views/

Kinderleher, D., & Stampacchia, G. (1980). *Variational inequalities and their applications*. New York: Academic Press.

Kirk, J. (2014). Target contractor says it was victim of cyberattack. *PC World*, February 6.

Koshal, J., Nedic, A., & Shanbhag, U.V. (2011). Multiuser optimization, distributed algorithms and error analysis. *SIAM Journal on Optimization*, 21(3), 1046-1081.

Lewis, D. (2014). Sony Pictures data breach and the PR Nightmare. *Forbes*, December 16.

Manshei, M.H., Zhu, Q., Alpcan, T., Basar, T., & Hubaux, J.-P. (2013). Game theory meets networks security and privacy. *ACM Computing Surveys*, 45(3), 25:1-25:39.

Nagurney, A. (1999). *Network economics: A variational inequality approach*, second and revised edition. Boston, Massachusetts: Kluwer Academic Publishers.

Nagurney, A. (2006). *Supply chain network economics: Dynamics of prices, flows, and profits*. Cheltenham, England: Edward Elgar Publishing.

Nagurney, A. (2015). A multiproduct network economic model of cybercrime in financial services. *Service Science*, 7(1), 70-81.

Nagurney, A., Nagurney, L.S., & Shukla, S. (2015). A supply chain game theory framework for cybersecurity investments under network vulnerability. In N. Daras and M. Th. Rassias (Eds.), *Computation, cryptography, and network security* (pp. 381-398). Switzerland: Springer International Publishing.

Nagurney, A., & Zhang, D. (1996). *Projected dynamical systems and variational inequalities with applications*. Boston, Massachusetts: Kluwer Academic Publishers.

Nash, J.F. (1950). Equilibrium points in n-person games. *Proceedings of the National Academy of Sciences, USA*, 36, 48-49.

Nash, J.F. (1951). Noncooperative games. *Annals of Mathematics*, 54, 286-298.

PricewaterhouseCoopers (2014a). Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015, September 30.

PricewaterhouseCoopers (2014b). US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US state of cybercrime survey. Retrieved from: http://www.pwc.com /us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Purnell, N. (2015). Cyberdefense spending rises amin high profile hacks. *The Wall Street Journal*, April 8, 2015.

Rue, R., Pfleeger, S.L., & Ortiz, D. (2007). A framework for classifying and comparing models of cyber security investment to support policy and decision-making. *Proceedings of The Sixth Workshop on the Economics of Information Security (WEIS 2007)*, Pittsburgh, Pennsylvania, June 7-8.

Shetty, N. G. (2010). Design of network architectures: Role of game theory and economics. PhD dissertation, Technical Report No. UCB/EECS-2010-91, Electrical Engineering and Computer Sciences, University of California at Berkeley, June 4.

Shetty, N., Schwartz, G., Felegehazy, M., & Walrand, J. (2009). Competitive cyber-insurance and Internet security. *Proceedings of The Eighth Workshop on the Economics of Information Security (WEIS 2009)*, University College London, England, June 24-25.

Toyasaki, F., Daniele, P., & Wakolbinger, T. (2014). A variational inequality formulation of equilibrium models for end-of-life products with nonlinear constraints. *European Journal of Operational Research*, 236, 340-350.

Yakowicz, W. (2014). Be prepared to up your cybersecurity budget. *Inc*, February 26.