A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability

Anna Nagurney, Ladimer S. Nagurney, and Shivani Shukla

In *Computation, Cryptography, and Network Security*, N.J. Daras and M.T. Rassias, Editors, Springer International Publishing Switzerland (2015), pp 381-398.

Abstract In this paper, we develop a supply chain game theory framework consisting of retailers and consumers who engage in electronic transactions via the Internet and, hence, may be susceptible to cyberattacks. The retailers compete noncooperatively in order to maximize their expected profits by determining their optimal product transactions as well as cybersecurity investments in the presence of network vulnerability. The consumers reveal their preferences via the demand price functions, which depend on the product demands and on the average level of security in the supply chain network. We prove that the governing Nash equilibrium conditions of this model can be formulated as a variational inequality problem, provide qualitative properties of the equilibrium product transaction and security investment pattern, and propose an algorithm with nice features for implementation. The algorithm is then applied to two sets of numerical examples that reveal the impacts on the equilibrium product transactions, the security levels, the product prices, the expected profits, and the retailer vulnerability as well as the supply chain network vulnerability, of such issues as: increased competition, changes in the demand price functions, and changes in the security investment cost functions.

Key words: supply chains, cybersecurity, investments, game theory, Nash equilibrium, variational inequalities, network vulnerability

---

Anna Nagurney
Department of Operations and Information Management, Isenberg School of Management, University of Massachusetts, Amherst, Massachusetts 01003, e-mail: nagurney@isenberg.umass.edu

Ladimer S. Nagurney
Department of Electrical and Computer Engineering, University of Hartford, West Hartford, Connecticut 06117, e-mail: nagurney@hartford.edu

Shivani Shukla
Department of Operations and Information Management, Isenberg School of Management, University of Massachusetts, Amherst, Massachusetts 01003, e-mail: sshukla@som.umass.edu

1 Introduction

As supply chains have become increasingly globalized and complex, there are new risks and vulnerabilities associated with their IT infrastructure due to a spectrum of cyberattacks with greater exposure for both firms and consumers. Coupled with cyberattacks are associated costs, in the form of financial damages incurred by the supply chain firms, the loss of their reputations, as well as opportunity costs, etc. Consumers may also be affected financially by cyberattacks and suffer from the associated disruptions. Cyberattacks can affect numerous different industrial sectors from financial services, energy providers, high tech firms, and retailers to the healthcare sector as well as governments. As noted in [16], the Center for Strategic and International Studies [3] 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, more than the national income of most countries.

For example, the 2013 breach of the major US-based retailer, Target, was accomplished when the cyberattacker entered a vulnerable supply chain link by exploiting the vulnerability in the remote diagnostics of the HVAC system supplier connected to the Target's IT system. In the attack, an estimated 40 million payment cards were stolen between November 27 and December 15, 2013 and upwards of 70 million other personal records compromised (cf. [10]). Target suffered not only financial damages but also reputational costs. Other cyber data breaches have occurred at the luxury retailer Neiman Marcus, the restaurant chain P.F. Changs, and the media giant Sony (cf. [17]). The Ponemon Institute [22] calculates that the average annualized cost of cybercrime for 60 organizations in their study is $11.6 million per year, with a range of $1.3 million to $58 million. According to The Security Ledger [25], cyber supply chain risk escapes notice at many firms. Mandiant [11] reports that 229 was the median number of days in 2013 that threat groups were present on a victim's network before detection.

Given the impact of cybercrime on the economy and society, there is great interest in evaluating cybersecurity investments. Each year $15 billion is spent by organizations in the United States to provide security for communications and information systems (see [8], [13]). Nevertheless, breaches due to cyberattacks continue to make huge negative economic impacts on businesses and society at-large. There is, hence, growing interest in the development of rigorous scientific tools that can help decision-makers assess the impacts of cybersecurity investments. What is essential to note, however, is that in many industries, including retail, investments by one decision-maker may affect the decisions of others and the overall supply chain network security (or vulnerability). Hence, a holistic approach is needed and some are even calling for a new discipline of cyber supply chain risk management ([2]).

In this paper, we develop a supply chain game theory model consisting of two tiers: the retailers and the consumers. The retailers select the product transactions and their security levels so as to maximize their expected profits. The probability of a successful attack on a retailer depends not only on that retailer's investment in security but also on the security investments of the other retailers. Hence, the retailers and consumers are connected. In our previous work (see [17]), we assumed

that the probability of a successful attack on a seller depended only on his own security investments. We know that in retail, which we consider in a broad sense here from consumer goods to even financial services, including retail banks, decision-makers interact and may share common suppliers, IT providers, etc. Hence, it is imperative to capture the network effects associated with security investments and the associated impacts.

In our model, retailers seek to maximize their expected profits with the prices that the consumers are willing to pay for the product being a function not only of the demand but also of the average security in the supply chain which we refer to as the cybersecurity or network security. The retailers compete noncooperatively until a Nash equilibrium is achieved, whereby no retailer can improve upon his expected profit by making a unilateral decision in changing his product transactions and security level. Our approach is inspired, in part, by the work of Shetty et al. [24], but it is significantly more general since the retailers, that is, the firms, are not identical and we explicitly also capture the demand side of the supply chain network. Moreover, the retailers may be faced with distinct security investment cost functions, given their existing IT infrastructure and business scope and size, and they can also be spatially separated. Our framework can handle both online retailers and brick and mortar ones. In addition, the retailers are faced with, possibly, different financial damages in the case of a cyberattack. For simplicity of exposition and clarity, we focus on a single type of attack. For a survey of game theory, as applied to network security and privacy, we refer the reader to Manshaei et al. [12]. For highlight of optimization models for cybersecurity investments, see [9].

The supply chain game theory model is developed in Section 2. The behavior of the retailers is captured, the Nash equilibrium defined and the variational inequality formulation derived. We also provide some qualitative properties of the equilibrium product transaction and security level pattern. In Section 3, we outline the algorithm that we then utilize in Section 4 to compute solutions to our numerical examples. In two sets of numerical supply chain network examples, we illustrate the impacts of a variety of changes on the equilibrium solution, and on the retailer and supply chain network vulnerability. In Section 5, we summarize our results and present the conclusions along with suggestions for future research.

2 The Supply Chain Game Theory Model of Cybersecurity Investments Under Network Vulnerability

In the model, we consider m retailers that are spatially separated and that sell a product to n consumers. The retailers may be online retailers, engaging with consumers through electronic commerce, and/or brick and mortar retailers. Since our focus is on cybersecurity, that is, network security, we assume that the transactions in terms of payments for the product occur electronically through credit cards and/or debit cards. Consumers may also conduct searches to obtain information through cyberspace. We emphasize that here we consider retailers in a broad sense, and they

may include consumer goods retailers, pharmacies, high technology product outlets, and even financial service firms as well as retail banks. The network topology of the supply chain model, which consists of a tier of retailers and a tier of consumers, is depicted in Figure 1.

Since the Internet is needed for the transactions between retailers and consumers to take place, network security is relevant. Each retailer in our model is susceptible to a cyberattack through the supply chain network since retailers may interact with one another as well as with common suppliers and also share consumers. The retailers may suffer from financial damage as a consequence of a successful cyberattack, losses due to identity theft, opportunity costs, as well as a loss in reputation, etc. Similarly, consumers are sensitive as to how secure their transactions are with the retailers.

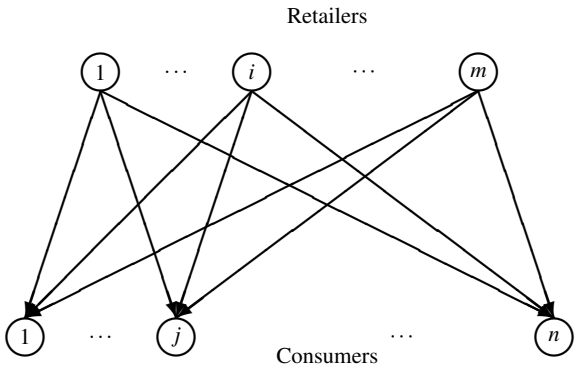

Fig. 1 The network structure of the supply chain game theory model

We denote a typical retailer by i and a typical consumer by j. Let Q_{ij} denote the nonnegative volume of the product transacted between retailer i and consumer j. Here s_i denotes the network security level, or, simply, the security of retailer i. The strategic variables of retailer i consist of his product transactions $\{Q_{i1}, \ldots, Q_{in}\}$ and his security level s_i. We group the product transactions of all retailers into the vector $Q \in R_+^{mn}$ and the security levels of all retailers into the vector $s \in R_+^m$. All vectors here are assumed to be column vectors, except where noted.

We have $s_i \in [0,1]$, with a value of 0 meaning no network security and a value of 1 representing perfect security. Therefore,

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

The network security level of the retail-consumer supply chain is denoted by $\bar{s}$ and is defined as the average network security where

$$\bar{s} = \frac{1}{m} \sum_{i=1}^{m} s_i. \tag{2}$$

Let p_i denote the probability of a successful cyberattack on retailer i in the supply chain network. Associated with the successful attack is the incurred financial damage D_i. Distinct retailers may suffer different amounts of financial damage as a consequence of a cyberattack due to their size and their existing infrastructure including cyber infrastructure. As discussed in [23] and [24], but for an oligopoly model with identical firms and no demand side represented in the network, p_i depends on the chosen security level s_i and on the network security level $\bar{s}$ as in (2). Using similar arguments as therein, we also define the probability p_i of a successful cyberattack on retailer i as

$$p_i = (1 - s_i)(1 - \bar{s}), \quad i = 1, \ldots, m, \tag{3}$$

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

In terms of cybersecurity investment, each retailer i, in order to acquire security s_i, encumbers an investment cost $h_i(s_i)$ with the function assumed to be continuously differentiable and convex. Note that distinct retailers, because of their size and existing cyber infrastructure (both hardware and software), may be faced with different investment cost functions. 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 (see [23, 24]). An example of a suitable $h_i(s_i)$ function is

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

The term α_i allows for different retailers to have distinct investment cost functions based on their size and needs.

The demand for the product by consumer j is denoted by d_j and it must satisfy the following conservation of flow equation:

$$d_j = \sum_{i=1}^{m} Q_{ij}, \quad j = 1, \ldots, n, \tag{5}$$

where

$$Q_{ij} \geq 0, \quad i = 1, \ldots, m; j = 1, \ldots, n, \tag{6}$$

that is, the demand for each consumer is satisfied by the sum of the product transactions between all the retailers with the consumer. We group the demands for the product for all buyers into the vector $d \in R^n_+$.

The consumers reveal their preferences for the product through their demand price functions, with the demand price function for consumer j, ρ_j, being:

$$\rho_j = \rho_j(d, \bar{s}), \quad j = 1, \ldots, n. \tag{7}$$

Observe that the demand price depends, in general, on the quantities transacted between the retailers and the consumers and the network security level. The consumers are only aware of the *average* network security level of the supply chain. This is reasonable since consumers may have information about a retail industry in terms of its cyber investments and security but it is unlikely that individual consumers would have information on individual retailers' security levels. Hence, as in the model of Nagurney and Nagurney [17], there is information asymmetry (cf. [1]).

In view of (2) and (5), we can define $\hat{\rho}_j(Q,s) \equiv \rho_j(d,\bar{s})$, $\forall j$. These demand price functions are assumed to be continuous, continuously differentiable, decreasing with respect to the respective consumer's own demand and increasing with respect to the network security level.

The revenue of retailer i; $i = 1,\ldots,m$, (in the absence of a cyberattack) is:

$$\sum_{j=1}^{n} \hat{\rho}_j(Q,s) Q_{ij}. \tag{8}$$

Each retailer i; $i = 1,\ldots,m$, is faced with a cost c_i associated with the processing and the handling of the product and transaction costs $c_{ij}(Q_{ij})$; $j = 1\ldots,m$, in dealing with the consumers. His total cost, hence, is given by:

$$c_i \sum_{j=1}^{n} Q_{ij} + \sum_{j=1}^{n} c_{ij}(Q_{ij}). \tag{9}$$

The transaction costs, in the case of electronic commerce, can include the costs of transporting/shipping the product to the consumers. The transaction costs can also include the cost of using the network services, taxes, etc. We assume that the transaction cost functions are convex and continuously differentiable.

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,

$$f_i(Q,s) = \sum_{j=1}^{n} \hat{\rho}_j(Q,s) Q_{ij} - c_i \sum_{j=1}^{n} Q_{ij} - \sum_{j=1}^{n} c_{ij}(Q_{ij}). \tag{10}$$

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

$$D_i p_i, \tag{11}$$

where D_i takes on a positive value.

Using expressions (3), (10), and (11), the expected utility, $E(U_i)$, of retailer i; $i = 1,\ldots,m$, which corresponds to his expected profit, is:

$$E(U_i) = (1-p_i) f_i(Q,s) + p_i(f_i(Q,s) - D_i) - h_i(s_i). \tag{12}$$

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 $K^i \equiv \{(Q_i, s_i) | Q_i \geq 0, \text{ and } 0 \leq s_i \leq 1\}$ 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^*) for which the m retailers will be in a state of equilibrium as defined below. Nash [20, 21] generalized Cournot's concept (see [4]) 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 $i; i = 1, \ldots, m$,

$$E(U_i(Q_i^*, s_i^*, \hat{Q}_i^*, \hat{s}_i^*)) \geq E(U_i(Q_i, s_i, \hat{Q}_i^*, \hat{s}_i^*)), \quad \forall (Q_i, s_i) \in K^i, \tag{13}$$

where

$$\hat{Q}_i^* \equiv (Q_1^*, \ldots, Q_{i-1}^*, Q_{i+1}^*, \ldots, Q_m^*); \quad \textit{and} \quad \hat{s}_i^* \equiv (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_m^*). \tag{14}$$

According to (13), an equilibrium is established if no retailer can unilaterally improve upon his expected profits by selecting an alternative vector of product transactions and security levels.

2.1 Variational Inequality Formulations

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

Theorem 1

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 continuous and 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

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

$$\forall (Q, s) \in K, \tag{15}$$

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

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

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

$$\forall (Q,s)\in K. \qquad (16)$$

Proof: (15) follows directly from Gabay and Moulin [7] and Dafermos and Nagurney [5].

In order to obtain variational inequality (16) from variational inequality (15), we note that, at the equilibrium:

$$-\frac{\partial E(U_i)}{\partial Q_{ij}}=c_i+\frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}}-\hat{\rho}_j(Q^*,s^*)-\sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*,s^*)}{\partial Q_{ij}}\times Q_{ik}^*;\quad \forall i,\forall j, \quad (17)$$

and

$$-\frac{\partial E(U_i)}{\partial s_i}=\frac{\partial h_i(s_i^*)}{\partial s_i}-(1-\sum_{j=1}^{m}\frac{s_j^*}{m}+\frac{1-s_i^*}{m})D_i-\sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*,s^*)}{\partial s_i}\times Q_{ik}^*;\quad \forall i. \quad (18)$$

Making the respective substitutions using (17) and (18) in variational inequality (15) yields variational inequality (16) □

We now put the above Nash equilibrium problem into standard variational inequality form, that is: determine $X^*\in\mathcal{K}\subset R^N$, such that

$$\langle F(X^*),X-X^*\rangle\geq 0,\quad \forall X\in\mathcal{K}, \qquad (19)$$

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

$$F_{ij}^1(X)\equiv-\frac{\partial E(U_i(Q,s))}{\partial Q_{ij}}, \qquad (20)$$

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

$$F_i^2(X)\equiv-\frac{\partial E(U_i(Q,s))}{\partial s_i}, \qquad (21)$$

and with the feasible set $\mathcal{K}\equiv K$. Then, clearly, variational inequality (15) can be put into standard form (19).

In a similar way, one can prove that variational inequality (16) can also be put into standard variational inequality form (19). □

Additional background on the variational inequality problem can be found in the books by Nagurney [14] and Nagurney et al. [19].

2.2 Qualitative Properties

It is reasonable to expect that the expected utility of any seller i, $E(U_i(Q,s))$, would decrease whenever his product volume has become sufficiently large, that is, when $E(U_i)$ is differentiable, $\frac{\partial E(U_i(Q,s))}{\partial Q_{ij}}$ is negative for sufficiently large Q_{ij} Hence, the following assumption is not unreasonable:

Assumption 1
Suppose that in our supply chain game theory model there exists a sufficiently large M, such that for any (i,j),

$$\frac{\partial E(U_i(Q,s))}{\partial Q_{ij}} < 0, \tag{22}$$

for all product transaction patterns Q with $Q_{ij} \geq M$.

We now give an existence result.

Proposition 1
Any supply chain Nash equilibrium problem in product transactions and security levels, as modeled above, that satisfies Assumption 1 possesses at least one equilibrium product transaction and security level pattern.

Proof: The proof follows from Proposition 1 in Zhang and Nagurney [26]. □

We now present the uniqueness result, the proof of which follows from the basic theory of variational inequalities (cf. [14]).

Proposition 2
Suppose that F is strictly monotone at any equilibrium point of the variational inequality problem defined in (19). Then it has at most one equilibrium point.

3 The Algorithm

For computational purposes, we will utilize the Euler method, which is induced by the general iterative scheme of Dupuis and Nagurney [6]. Specifically, iteration τ of the Euler method (see also [14]) is given by:

$$X^{\tau+1} = P_{\mathscr{K}}(X^{\tau} - a_{\tau}F(X^{\tau})), \tag{23}$$

where $P_{\mathscr{K}}$ is the projection on the feasible set $\mathscr{K}$ and F is the function that enters the variational inequality problem (19).

As proven in [6], 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 $\tau \rightarrow \infty$. Specific conditions for convergence of this scheme as well as various applications to the solutions of other network-based game theory models can be found in [15], [16], and the references therein.

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

The elegance of this procedure 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 $i = 1, \ldots, m; j = 1, \ldots, n$:

$$Q_{ij}^{\tau+1} = \max\{0, Q_{ij}^{\tau} + a_\tau(\hat{\rho}_j(Q^\tau, s^\tau) + \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^\tau, s^\tau)}{\partial Q_{ij}} Q_{ik}^{\tau} - c_i - \frac{\partial c_{ij}(Q_{ij}^{\tau})}{\partial Q_{ij}})\}, \quad (24)$$

and the following closed form expression for the security levels $i = 1, \ldots, m$:

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

$$\max\{0, \min\{1, s_i^{\tau} + a_\tau(\sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^\tau, s^\tau)}{\partial s_i} Q_{ik}^{\tau} - \frac{\partial h_i(s_i^{\tau})}{\partial s_i} + (1 - \sum_{j=1}^{m} \frac{s_j}{m} + \frac{1 - s_i}{m}) D_i)\}\}. \quad (25)$$

We now provide the convergence result. The proof is direct from Theorem 5.8 in [19].

Theorem 2

In the supply chain game theory model developed above let $F(X) = -\nabla E(U(Q,s))$ be strictly monotone at any equilibrium pattern and assume that Assumption 1 is satisfied. Also, assume that F is uniformly Lipschitz continuous. Then there exists a unique equilibrium product transaction and security level pattern $(Q^*, s^*) \in K$ and any sequence generated by the Euler method as given by (23), with $\{a_\tau\}$ satisfies $\sum_{\tau=0}^{\infty} a_\tau = \infty$, $a_\tau > 0$, $a_\tau \rightarrow 0$, as $\tau \rightarrow \infty$ converges to (Q^*, s^*).

In the next Section, we apply the Euler method to compute solutions to numerical game theory problems.

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 $\varepsilon = 10^{-4}$. Hence, 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 $Q_{ij} = 1.00, \forall i, j$, and the security level of each retailer $s_i = 0.00, \forall i$.

We present two sets of numerical examples. Each set of examples consists of an example with four variants.

Example Set 1

The first set of examples consists of two retailers and two consumers as depicted in Figure 2. This set of examples begins with the baseline Example 1, followed by four variants. The equilibrium solutions are reported in Table 1.

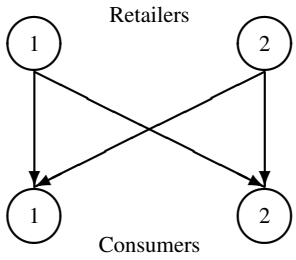

Fig. 2 Network Topology for Example Set 1

The cost function data for Example 1 are:

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

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

The demand price functions are:

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

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

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

As can be seen from the results in Table 1 for Example 1, the equilibrium demand for Consumer 2 is over 4 times greater than that for Consumer 1. The price that Consumer 1 pays is about one half of that of Consumer 2. Both retailers invest in security and achieve equilibrium security levels of .91. Hence, in Example 1 the vulnerability of Retailer 1 is .09 and that of Retailer 2 is also .09, with the network vulnerability being .09.

In the first variant of Example 1, Variant 1.1, we change the demand price function of Consumer 1 to reflect an enhanced willingness to pay more for the product. The new demand price function for Consumer 1 is:

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

The product transactions to Consumer 1 more than double from their corresponding values in Example 1, whereas those to Consumer 2 remain unchanged. The security level of Retailer 2 increases slightly whereas that of Retailer 1 remains unchanged. Both retailers benefit from increased expected profits. The vulnerability of Retailer 2 is decreased slightly to .08.

Variant 1.2 is constructed from Variant 1.1. Consumer 2 no longer values the product much so his demand price function is

$$\rho_2(d_2, \bar{s}) = -.5d_2 + .2(\frac{s_1 + s_2}{2}) + 20,$$

with the remainder of the data as in Variant 1.1. The product transactions decrease by almost an order of magnitude to the second consumer and the retailers experience reduced expected profits by about 2/3 as compared to those in Variant 1.1. The vulnerability of Retailer 1 is now .12 and that of Retailer 2: .11 with the network vulnerability being: .115.

Variant 1.3 is constructed from Example 1 by increasing both security investment cost functions so that:

$$h_1(s_1) = 100(\frac{1}{\sqrt{(1-s_1)}} - 1), \quad h_2(s_2) = 100(\frac{1}{\sqrt{(1-s_2)}} - 1)$$

and having new damages: $D_1 = 500$ and $D_2 = 700$. With the increased costs associated with cybersecurity investments both retailers decrease their security levels to the lowest level of all the examples solved, thus far. The vulnerability of Retailer 1 is now .34 and that of Retailer 2: .28 with the network vulnerability =.31.

Variant 1.4 has the same data as Variant 1.3, but we now further increase Retailer 2's investment cost function as follows:

$$h_2(s_2) = 1000(\frac{1}{\sqrt{(1-s_2)}} - 1).$$

Retailer 2 now has an equilibrium security level that is one quarter of that in Variant 1.3. Not only do his expected profits decline but also those of Retailer 1 do.

The vulnerability of Retailer 1 is now: .27 and that of Retailer 2: .82. The network vulnerability for this example is: .54, the highest value in this set of examples. The cybersecurity investment cost associated with Retailer 2 is so high that he greatly reduces his security level. Moreover, the network security is approximately half of that obtained in Example 1.

Table 1 Equilibrium Solutions for Examples in Set 1

Solution	Ex. 1	Var. 1.1	Var. 1.2	Var. 1.3	Var. 1.4
Q_{11}^*	24.27	49.27	49.27	24.27	24.26
Q_{12}^*	98.30	98.30	8.30	98.32	98.30
Q_{21}^*	21.27	46.27	46.27	21.27	21.26
Q_{22}^*	93.36	93.36	3.38	93.32	93.30
d_1^*	45.55	95.55	95.55	45.53	45.52
d_2^*	191.66	191.66	11.68	191.64	191.59
s_1^*	.91	.91	.88	.66	.73
s_2^*	.91	.92	.89	.72	.18
$\bar{s}^*$	.91	.915	.885	.69	.46
$\rho_1(d_1^*, \bar{s}^*)$	54.55	104.55	104.54	54.54	54.52
$\rho_2(d_2^*, \bar{s}^*)$	104.35	104.35	14.34	104.32	104.30
$E(U_1)$	8136.45	10894.49	3693.56	8121.93	8103.09
$E(U_2)$	7215.10	9748.17	3219.94	7194.13	6991.11

Example Set 2

The second set of numerical examples consists of three retailers and two consumers as shown in Figure 3.

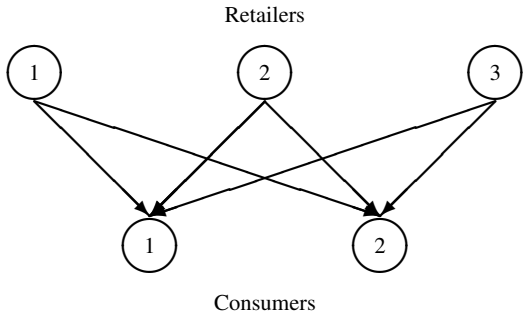

Fig. 3 Network Topology for Example Set 2

In order to enable cross comparisons between the two example sets, we construct Example 2, which is the baseline example in this set, from Example 1 in Set 1. Therefore, the data for Example 2 is identical to that in Example 1 except for the new Retailer 3 data as given below:

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

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

Also, since there are now 3 retailers, the demand price functions become:

$$\rho_1(d,\bar{s}) = -d_1 + .1(\frac{s_1+s_2+s_3}{3}) + 100, \quad \rho_2(d,\bar{s}) = -.5d_2 + .2(\frac{s_1+s_2+s_3}{3}) + 200.$$

The equilibrium solutions for examples in Set 2 are reported in Table 2. With the addition of Retailer 3, there is now increased competition. As a consequence, the demand prices for the product drop for both consumers 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 Consumer 1 and also for Consumer 2, both at upwards of 10%.

The vulnerability of Retailer 1 is .10, that of Retailer 2: .09, and that of Retailer 3: .19 with a network vulnerability of: .13. 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.

Variant 2.1 is constructed from Example 2 with the data as therein except for the new demand price function for Consumer 1, who now is more sensitive to the network security, where

$$\rho_1(d_1,\bar{s}) = -d_1 + (\frac{s_1+s_2+s_3}{3}) + 100.$$

The expected profit increases for all retailers since Consumer 1 is willing to pay a higher price for the product.

The vulnerability of Retailer 1 is now .08, that of Retailer 2: .08, and that of Retailer 3: .17 with a network vulnerability of: .11. Hence, all the vulnerabilities have decreased, since the retailers have higher equilibrium security levels.

Variant 2.2 is constructed from Variant 2.1. The only change is that now Consumer 2 is also more sensitive to average security with a new demand price function given by:

$$\rho_2(d_2,\bar{s}) = -.5d_2 + (\frac{s_1+s_2+s_3}{3}) + 200.$$

As shown in Table 2, the expected profits are now even higher than for Variant 2.1. The vulnerability of Retailer 1 is now .05, which is the same for Retailer 2, and with Retailer 3 having the highest vulnerability at: .14. The network vulnerability is, hence, .08. Consumers' willingness to pay for increased network security reduces the retailers' vulnerability and that of the supply chain network.

Variants 2.1 and 2.2 demonstrate that consumers who care about security can also enhance the expected profits of retailers of a product through their willingness to pay for higher network security.

Variant 2.3 has the identical data to that in Variant 2.2 except that the demand price functions are now:

$$\rho_1(d_1,\bar{s}) = -2d_2 + (\frac{s_1+s_2+s_3}{3}) + 100, \quad \rho_2(d_2,\bar{s}) = -d_2 + (\frac{s_1+s_2+s_3}{3}) + 100.$$

As can be seen from Table 2, the product transactions have all decreased substantially, as compared to the respective values for Variant 2.2. Also, the demand

prices associated with the two consumers have decreased substantially as have the expected profits for all the retailers.

The vulnerabilities of the retailers are, respectively: .07, 07, and .16 with the network vulnerability equal to .10.

Variant 2.4 is identical to Variant 2.3 except that now the demand price function sensitivity for the consumers has increased even more so that:

$$\rho_1(d_1,\bar{s}) = -2d_2 + 10(\frac{s_1+s_2+s_3}{3}) + 100, \quad \rho_2(d_2,\bar{s}) = -d_2 + 10(\frac{s_1+s_2+s_3}{3}) + 100.$$

All the equilibrium product transactions now increase. The demand prices have both increased as have the expected profits of all the retailers.

In this example, the vulnerabilities of the retailers are, respectively: .02, .02, and .05, yielding a network vulnerability of .03. This is the least vulnerable supply chain network in our numerical study.

Table 2 Equilibrium Solutions for Examples in Set 2

Solution	Ex. 2	Var. 2.1	Var. 2.2	Var. 2.3	Var. 2.4
Q_{11}^*	20.80	20.98	20.98	11.64	12.67
Q_{12}^*	89.45	89.45	89.82	49.62	51.84
Q_{21}^*	17.81	17.98	17.98	9.64	10.67
Q_{22}^*	84.49	84.49	84.83	46.31	48.51
Q_{31}^*	13.87	13.98	13.98	8.73	9.50
Q_{32}^*	35.41	35.41	35.53	24.50	25.59
d_1^*	52.48	52.94	52.95	30.00	32.85
d_2^*	209.35	209.35	210.18	120.43	125.94
s_1^*	.90	.92	.95	.93	.98
s_2^*	.91	.92	.95	.93	.98
s_3^*	.81	.83	.86	.84	.95
$\bar{s}^*$	.87	.89	.917	.90	.97
$\rho_1(d_1^*,\bar{s}^*)$	47.61	47.95	47.96	40.91	44.01
$\rho_2(d_2^*,\bar{s}^*)$	95.50	95.50	95.83	80.47	83.77
$E(U_1)$	6654.73	6665.88	6712.29	3418.66	3761.75
$E(U_2)$	5830.06	5839.65	5882.27	2913.31	3226.90
$E(U_3)$	2264.39	2271.25	2285.93	1428.65	1582.62

5 Summary and Conclusions

Cybercrime is affecting companies as well as other organizations and establishments, including governments, and consumers. Recent notable data breaches have included major retailers in the United States, resulting in both financial damage and a loss in reputation. With companies, many of which are increasingly global and dependent on their supply chains, seeking to determine how much they should invest

in cybersecurity, a general framework that can quantify the investments in cybersecurity in supply chain networks is needed. The framework should also be able to illuminate the impacts on profits as well as a firm's vulnerability and that of the supply chain network.

In this paper, we develop a supply chain network game theory model consisting of a tier of retailers and a tier of consumers. 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 firms compete noncooperatively until a Nash equilibrium is achieved, whereby no retailer can improve upon his expected profits. 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 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 derive the variational inequality formulation of the governing equilibrium conditions, discuss qualitative properties, and demonstrate that the algorithm that we propose has nice features for computations. Specifically, it yields, at each iteration, closed form expressions for the product transactions between retailers and consumers and closed form expressions for the retailer security levels. The algorithm is then applied to compute solutions to two sets of numerical examples, with a total of ten examples. 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 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 approach of applying game theory and variational inequality theory with expected utilities of decision-makers to network security / cybersecurity that this paper adopts is original in itself. 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. The complexity of the supply chain network would then make it even more susceptible to cyberattacks, wherein a security lapse in one node can affect many others in succession. Moreover, to account for the fact that the exchange of data takes place through multiple forms, the model could be extended to include multiple modes of transactions.

While the solution equilibrium in the context of competition does moderate investments, the model can also be extended to explicitly include constraints on cybersecurity investments subject to expenditure budgets allocated to cybersecurity. The numerical examples section dealt with multiple retailer and consumer scenarios and their variants to validate the ease of adoption and practicality of the model. A case study and empirical analysis can further corroborate the cogency of the model and assist in the process of arriving at investment decisions related to cybersecurity. This could also provide insights as to how to strike a balance between effectiveness of service and security. 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.

References

1. Akerlof, G.A.: The market for lemons: Quality uncertainty and the market mechanism. Quarterly Journal of Economics, 84(3), 488-500 (1970)
2. Boyson, S.: Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation 34(7), 342-353 (2014)
3. Center for Strategic and International Studies: Net losses: Estimating the global cost of cybercrime. Santa Clara, California (2014)
4. Cournot, A. A.: Researches into the Mathematical Principles of the Theory of Wealth, English translation. London, England: MacMillan (1838)
5. Dafermos S., Nagurney, A.: Oligopolistic and competitive behavior of spatially separated markets. Regional Science and Urban Economics, 17, 245-254 (1987)
6. Dupuis, P., Nagurney, A.: Dynamical systems and variational inequalities. Annals of Operations Research, 44, 9-42 (1993)
7. Gabay, D., Moulin, H.: On the uniqueness and stability of Nash equilibria in noncooperative games. In Bensoussan, A., Kleindorfer, P., & Tapiero, C. S. (Ed.), Applied Stochastic Control of Econometrics and Management Science. Amsterdam, The Netherlands: North-Holland (1980)
8. Gartner: Gartner reveals Top 10 Security Myths, by Ellen Messmer, NetworkWorld, June 11 (2013)
9. Gordon, L.A., Loeb1, M.P., Lucyshyn, W., Zhou, L.: Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. Journal of Information Security, 6, 24-30 (2015)
10. Kirk, J.: Target contractor says it was victim of cyberattack. PC World, February 6 (2014)
11. Mandiant: M-trends: Beyond the breach. 2014 threat report. Alexandria, Virginia (2014)
12. Manshei, M.H., Alpcan, T., Basar, T., Hubaux, J.-P. Game theory meets networks security and privacy. ACM Computing Surveys, 45(3, June (2013)
13. Market Research: United States Information Technology Report Q2 2012, April 24 (2013)
14. Nagurney, A.. Network Economics: A Variational Inequality Approach, second and revised edition. Boston, Massachusetts: Kluwer Academic Publishers (199)
15. Nagurney, A.: Supply Chain Network Economics: Dynamics of Prices, Flows, and Profits. Edward Elgar Publishing. Cheltenham, England (2006)
16. Nagurney, A.: A multiproduct network economic model of cybercrime in financial services. Service Science, 7(1), 70-81 (2015)
17. Nagurney, A., Nagurney, L.S.: A game theory model of cybersecurity investments with information asymmetry. Netnomics, in press (2015)
18. Nagurney, A., Yu, M., Masoumi, A.H., Nagurney, L.S.: Networks Against Time: Supply Chain Analytics for Perishable Products. Springer Business + Science Media, New York (2013)
19. Nagurney, A., Zhang, D.: Projected Dynamical Systems and Variational Inequalities with Applications. Kluwer Academic Publishers, Boston, Massachusetts (1996)
20. Nash, J.F.: Equilibrium points in n-person games. Proceedings of the National Academy of Sciences, USA, 36, 48-49 (1950)
21. Nash, J.F.: Noncooperative games. Annals of Mathematics, 54, 286-298 (1951)

22. Ponemon Institute: Second annual cost of cyber crime study: benchmark study of U.S. companies (2013)
23. Shetty, N.G.: 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 (2010)
24. Shetty, N., Schwartz, G., Felegehazy, M., Walrand, J.: Competitive cyber-insurance and Internet security. Proceedings of the The Eighth Workshop on the Economics of Information Security (WEIS 2009) University College London, England, June 24-25 (2009)
25. The Security Ledger: Supply chain risk escapes notice at many firms. November 6 (2014)
26. Zhang, D., Nagurney, A.: On the stability of projected dynamical systems. Journal of Optimization Theory and its Applications, 85, 97-124 (1995).