A Game Theory Model of Cybersecurity Investments with Information Asymmetry

Anna Nagurney
Isenberg School of Management
University of Massachusetts, Amherst, Massachusetts 01003
and
Ladimer S. Nagurney
Department of Electrical and Computer Engineering
University of Hartford, West Hartford, Connecticut 06117

January 2015; revised March and April 2015
Netnomics (2015), **16(1-2)**, pp 127-148.

Abstract:

In this paper, we develop a game theory model consisting of sellers and buyers with sellers competing non-cooperatively in order to maximize their expected profits by determining their optimal product transactions as well as cybersecurity investments. The buyers reflect their preferences through the demand price functions, which depend on the product demands and on the average level of security in the marketplace. We demonstrate that the governing equilibrium conditions of this model with security information asymmetry can be formulated as a variational inequality problem. We provide qualitative properties and propose an algorithmic scheme that is easy to implement. Three sets of numerical examples are presented which reveal the impacts of the addition of buyers and sellers and a variety of changes in demand price and investment cost functions on the equilibrium product transaction and security level patterns.

Key words: cybersecurity, investments, game theory, Nash equilibrium, information asymmetry, variational inequalities

1. Introduction

While the Internet has revolutionized the manner in which we conduct many business transactions, obtain information and entertainment, and even communicate, it has, nevertheless, led to new pathways for cyber hacking and cybercrime. According to the Center for Strategic and International Studies [5] the estimated annual cost to the world-wide economy from cybercrime is more than $400 billion with a conservative estimate being $375 billion in losses, exceeding the national income of most countries.

Recent examples of dramatic cyber attacks that have garnered much media attention have included the security breach at the retail giant Target with an estimated 40 million payment cards stolen between November 27 and December 15, 2013 and upwards of 70 million other personal records compromised ([13]). This led not only to financial damages for Target but also to reputational costs. Other cyber data breaches have occurred at the luxury retailer Neiman Marcus, the restaurant chain P.F. Chang's, and the media giant Sony. The Ponemon Institute [27] determined 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 Alter [2], the first three months of 2014, revealed 254 reports of data breaches, resulting in more than 200 million data records lost or stolen. This represents a 233% year-over-year increase, according to data security company SafeNet. Alter [2] reports that records were lost or stolen in the first quarter of 2014 at an alarming rate of 70 million every month, 2 million every day, and 93,000 every hour.

However, it is important to emphasize that the impact of cybercrime affects industries and economic sectors differently. As noted in [19], the PriceWaterhouseCoopers 2014 Global Economic Crime Survey [28] reports that 39% of financial sector respondents said that they had been victims of cybercrime, compared with only 17% in other industries, with cybercrime now the second most commonly reported economic crime affecting financial services firms. The healthcare sector, technology companies, and the government are also top targets of cyber attackers.

The realities of the cybercrime economic landscape calls for rigorous treatment and analysis of cybersecurity investments. According to Market Research [16] and Gartner [10], $15 billion is spent each year by organizations in the United States to provide security for communications and information systems. The real-world recognition of the importance of cybersecurity investments has also drawn attention in the research literature. We note the well-known security investment model of Gordon and Loeb [11], which utilizes a security breach probability function, with the authors deriving a rule for determining security in-

vestment in the case of a single decision-maker. Extensions and variants have included the work of Hausken [12] who constructed different breach functions, that of Matsuura [17], who endogenized the probability of an attack, and Tatsumi and Goto [31, who focused on the timing of cybersecurity investments.

Nevertheless, breaches due to cyber attacks continue to make immense negative economic impacts on businesses and society at-large. This calls for the development of new, rigorous models that capture the competitive behavior of sellers and buyers in the modern marketplace along with cybersecurity investments. Anderson and Moore [3] emphasize live research challenges in the economics of information security and note that the discipline "is still young." Furthermore, they recognize the issue of information asymmetry in the software cybersecurity market. Background on information asymmetry can be found in the Nobel laureate George Akerlof's classic paper, which focused on quality, however, rather than security (see [1]). See also [20] for a network-based game theory model with information asymmetry and minimum quality standards and the references therein.

In particular, game theory holds promise as both a conceptual and methodological framework for the investigation of decision-makers who compete for business and need to determine the level of their cybersecurity investments so as to minimize potential financial damages due to cyber attacks. Cavusoglu, Raghunathan, and Yue [4] compare decision-theoretic and game-theoretic approaches to IT security investment, focusing on a firm and a hacker. Kunreuther and Heal [14], on the other hand, consider game theory for interdependent security, but the decisions are discrete, that is, whether to invest or not and describe applications of their framework to cybersecurity investments. They also assume, in contrast to our model, that all the decision-makers are identical. Varian [32] also utilized game theory to study interdependence among security firms' risks. For a survey of game theory, as applied to network security and privacy, we refer the reader to Manshaei et al. [15]. Therein, the authors emphasize that the application of game theory with incomplete and imperfect information is an emerging field in network security and privacy, with only a few papers published so far. In this paper we hope to, in part, fill this void.

Specifically, in this paper, we develop a game theory framework consisting of sellers of a product and buyers who engage in electronic transactions during the purchases of the product. In our setting, the product can correspond to a manufactured product, a financial product, or even a digital one. All that needs to transpire is that buyers utilize the Internet to engage in economic transactions, which could involve also credit or debit cards. Another essential component of our game theory model is information asymmetry in that individual sellers are aware of their investment in cybersecurity, whereas the buyers are only aware of

the average security of the sellers. The sellers in our model seek to maximize their expected profits while investing in security and competing amongst themselves. Buyers reflect their preferences through their demand price functions which depend on the product demands as well as the average security level for the marketplace. The governing concept is that of Nash equilibrium.

The literature on the economics of cybersecurity in terms of information asymmetry focuses on asymmetry associated with insurance in that insurers may not have complete information, unlike the sellers (cf. Shetty [29], Shetty et al. [30], and the references therein). Our game theory model, in contrast, considers information asymmetry between sellers of a product and buyers of the product. Moreover, unlike the former models, we do not assume that the sellers are identical nor are they faced with the same cybersecurity investment cost functions. Our contributions in the paper are as follows:

1). We develop a rigorous framework that captures competition among sellers in an oligopolistic market of non-identical sellers, who identify optimal product quantities as well as optimal cybersecurity investments;

2). We, for the first time, model information asymmetry associated with cybersecurity investments between buyers and sellers of a product;

3). Our model is not limited to specific functional forms for the seller transaction cost functions and the buyer demand price functions.

4). Our framework is computationally tractable and supported by both theoretical qualitative results and an algorithm, which enables the exploration of numerous sensitivity analysis experiments.

We develop the model in Section 2, state the equilibrium conditions, and derive the equivalent variational inequality formulation. We also provide some qualitative properties of the solution in terms of existence and uniqueness. In Section 3, we propose the algorithmic scheme, along with convergence results. The algorithm yields closed form expressions for the product transactions between buyers and sellers and the seller security levels at each iteration. In Section 4, we illustrate the game theory model via three sets of numerical examples, accompanied by sensitivity analysis, and managerial insights. A summary of results with conclusions is presented in Section 5.

2. The Game Theory Model of Cybersecurity Investments with Information Asymmetry

We consider m competitive sellers of a homogeneous product and n buyers as depicted in Figure 1. The buyers of the product are involved in electronic transactions associated with the purchase of the product, which can occur online and/or in a brick and mortar establishment through electronic processing of credit card or debit card payments. The buyers can be consumers of a product or those purchasing it for resale. In the case of electronic product purchases the sellers can correspond to a marketplace such as Amazon.com or a specific seller's website. The framework is also relevant to electronic finance, e.g., banking, with the sellers being those who offer a financial product and buyers being those who use that product. What is important in our framework is that the Internet is needed for the transactions between buyers and sellers to take place. Hence, network security is relevant since sellers can sustain financial damage as a consequence of a successful cyber attack encompassing the loss of a seller's reputation, losses due to identity theft, opportunity costs, etc. Similarly, buyers care about how secure their transactions are with the sellers. Here we use *network security* interchangeably with *cybersecurity*.

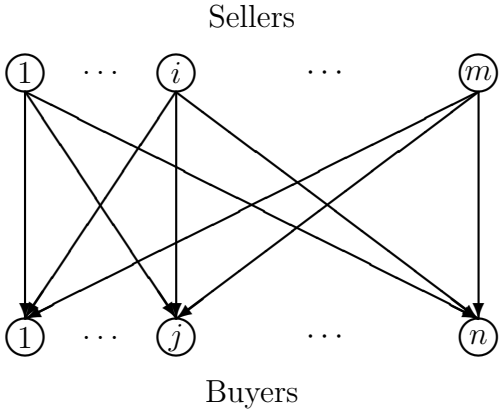

Figure 1: The network structure of the game theory model

We denote a typical seller by i and a typical buyer by j. Let Q_{ij} denote the nonnegative volume of the product transacted between seller i and buyer j. We group the product transactions into the vector $Q \in R_+^{mn}$. Here s_i denotes the network security level, or, simply, the security of seller i. We group the security levels of all sellers 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. Hence,

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

The strategic variables of seller i; $i = 1, \ldots, m$, are his product transactions $\{Q_i\}$ where $Q_i = (Q_{i1}, \ldots, Q_{in})$ and his security level s_i.

The average network security of the marketplace system is denoted by $\bar{s}$, where

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

We define the probability p_i of a successful cyber attack on seller i as

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

with notice that if a seller i has no security, then $p_i = 1$, and if he has perfect security then $p_i = 0$.

For each seller i, to achieve security s_i encumbers an investment cost $h_i(s_i)$ with the function assumed to be continuously differentiable and convex. Note that distinct sellers, because of their size and existing cyber infrastructure (both hardware and software), will be faced with different investment cost functions. We assume that, for a given seller i, $h_i(0) = 0$ denotes an entirely insecure seller and $h_i(1) = \infty$ is the investment cost associated with complete security for the seller (see Shetty [29], Shetty et al. [30]). An example of a suitable $h_i(s_i)$ function is $h_i(s_i) = \alpha_i(\frac{1}{\sqrt{(1-s_i)}} - 1)$ with $\alpha_i > 0$.

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

$$d_j = \sum_{i=1}^{m} Q_{ij}, \quad j = 1, \ldots, n, \tag{4}$$

where

$$Q_{ij} \geq 0, \quad i = 1, \ldots, m; j = 1, \ldots, n, \tag{5}$$

that is, the price that each buyer is willing to pay for the product depends, in general, on his own demand and that of the other buyers', as well as on the average security level in the marketplace. We group the demands for the product for all buyers into the vector $d \in R_+^n$.

The buyers reflect their preferences through their demand price functions, with the demand price function for buyer j, ρ_j, being as follows:

$$\rho_j = \rho_j(d, \bar{s}), \quad j = 1, \ldots, n. \tag{5}$$

Observe that in our model there is information asymmetry in that the buyers are only aware of an *average* security level of the marketplace, in general. This is reasonable since one may

have information about an industry in terms of its cyber investments and security but it is unlikely that individual buyers would have information on individual sellers' security levels.

In view of (2) and (4), 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 buyer's own demand and increasing with respect to the average security level.

Each seller 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 $c_{ij}(Q_{ij})$; $j = 1 \ldots, m$, with his total cost given by:

$$c_i \sum_{j=1}^{n} Q_{ij} + \sum_{j=1}^{n} c_{ij}(Q_{ij}). \tag{6}$$

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

Since the revenue of seller i (in the absence of a cyber attack) is:

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

we can express the profit f_i of seller i; $i = 1, \ldots, m$ (in the absence of a cyber attack and security investment) as the difference between the revenue and his costs, that is,

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

A seller i; $i = 1, \ldots, m$, incurs an expected financial damage if there is a successful cyber attack represented by

$$D_i p_i, \tag{9}$$

where D_i takes on a positive value.

Using the above expressions (3), (8), and (9), we can express the expected utility, $E(U_i)$, of seller i; $i = 1, \ldots, m$, which corresponds to his expected profit, as:

$$E(U_i) = (1 - p_i) f_i(Q, s) + p_i(f_i(Q, s) - D_i) - h_i(s_i). \tag{10}$$

We group the expected utilities of all the sellers 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 seller i, where $K^i \equiv \{(Q_i, s_i) | Q_i \geq 0, \text{ and } 0 \leq s_i \leq 1\}$ and define $K \equiv \prod_{i=1}^{m} K^i$.

We consider the competitive market mechanism in which the m sellers supply the product and invest in cybersecurity in a non-cooperative manner, 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 sellers will be in a state of equilibrium as defined below. In particular, Nash [25, 26] generalized Cournot's concept (cf. [6]) of an equilibrium for a model of several players, each of which acts in his/her own self-interest, in what is called a non-cooperative game.

Definition 1: Nash Equilibrium in Product Transactions and Security Levels

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

$$E(U_i(Q_i^*, s_i^*, \hat{Q}_i^*, \hat{s}_i^*)) \geq E(U_i(Q_i, s_i, \hat{Q}_i^*, \hat{s}_i^*)), \quad \forall (Q_i, s_i) \in K^i, \tag{11}$$

where

$$\hat{Q}_i^* \equiv (Q_1^*, \ldots, Q_{i-1}^*, Q_{i+1}^*, \ldots, Q_m^*); \quad \textit{and} \quad \hat{s_i^*} \equiv (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_m^*). \tag{12}$$

According to (11), an equilibrium is established if no seller 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 Nash equilibrium in product transactions and security levels.

Theorem 1

Assume that, for each seller 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 Nash equilibrium according to Definition 1 if and only if it satisfies the variational inequality

$$-\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} \times (Q_{ij} - Q_{ij}^*) - \sum_{i=1}^{m} \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0, \quad \forall (Q, s) \in K, \tag{13}$$

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

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

$$+\sum_{i=1}^{m}\left[\frac{\partial h_i(s_i^*)}{\partial s_i} - D_i - \sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q_{ik}^*\right] \times (s_i - s_i^*) \geq 0, \quad \forall (Q, s) \in K. \tag{14}$$

Proof: (13) follows directly from Gabay and Moulin [9] and Dafermos and Nagurney [7].

In order to obtain variational inequality (14) from variational inequality (13), we note that, at the equilibrium:

$$-\frac{\partial E(U_i)}{\partial Q_{ij}} = c_i + \frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} \times Q_{ik}^*; \quad i = 1, \ldots, m; j = 1, \ldots, n; \tag{15}$$

and

$$-\frac{\partial E(U_i)}{\partial s_i} = \frac{\partial h_i(s_i^*)}{\partial s_i} - D_i - \sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q_{ik}^*; \quad i = 1, \ldots, m. \tag{16}$$

Multiplying the right-most expression in (15) by $(Q_{ij} - Q_{ij}^*)$ and summing the resultant over all i and all j; similarly, multiplying the right-most expression in (16) by $(s_i - s_i^*)$ and summing the resultant over all i yields, respectively:

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\left[c_i + \frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} \times Q_{ik}^*\right] \times (Q_{ij} - Q_{ij}^*), \ \forall Q \in R_+^{mn} \tag{17}$$

and

$$\sum_{i=1}^{m}\left[\frac{\partial h_i(s_i^*)}{\partial s_i} - D_i - \sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q_{ik}^*\right] \times (s_i - s_i^*), \quad \forall s_i \in [0, 1], \forall i. \tag{18}$$

Finally, summing (17) and (18) and then using constraints (1) and (2), yields variational inequality (14). □

We now put the above Nash equilibrium problem into standard variational inequality form (see Nagurney [18]), that is: determine $X^* \in \mathcal{K} \subset R^N$, such that

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

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 row vector $F(X) = (F^1(X), F^2(X))$ with the (i, j)-th component, F^1_{ij}, of $F^1(X)$ given by

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

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

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

and with the feasible set $\mathcal{K} \equiv K$. Then, clearly, variational inequality (13) can be put into standard form (19).

In a similar manner, one can establish that variational inequality (14) can also be put into standard variational inequality form (19).

For additional background on the variational inequality problem, we refer the reader to the book by Nagurney [12].

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 reasonable:

Assumption 1

Suppose that in our 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 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 [33]. □

We now present the uniqueness result, the proof of which follows from the basic theory of variational inequalities (cf. [18]).

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 [8]. Specifically, iteration τ of the Euler method (see also [24]) is given by:

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

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

As shown 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 [21] – [24].

Explicit Formulae for the Euler Method Applied to the 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 $i = 1, \ldots, m; j = 1, \ldots, n$:

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

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

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

We now provide the convergence result. The proof is direct from Theorem 5.8 in Nagurney and Zhang (1996).

Theorem 2

In the game theory model described 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) above, where $\{a_\tau\}$ 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 described in Section 3, using FORTRAN on a Linux system at the University of Massachusetts Amherst. The convergence criterion was $\epsilon = 10^{-4}$; that is, 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 algorithm by setting each product transaction $Q_{ij} = 1.00$, $\forall i, j$, and by setting the security level of each supplier $s_i = 0.00$, $\forall i$.

We now present three sets of examples in order to illustrate both the model and the algorithm. Each set of examples consists of an example with four variants, followed by sensitivity analysis.

Example Set 1

The first set of examples consists of two sellers and a single buyer 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. We then include additional results in the form of sensitivity analysis on the demand price functions which we depict in graphical form in Figure 3.

The cost and demand price function data for Example 1 are:

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

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

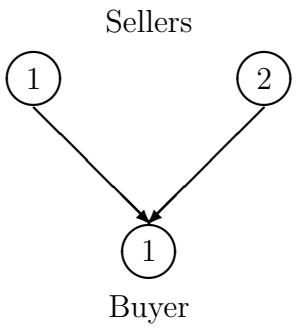

Figure 2: Network Topology for Example Set 1

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

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

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

From Table 1, one can see that Seller 1 sells more of the product than Seller 2 to the buyer and has a higher expected profit. His security level, however, is lower than that of Seller 2. The buyer is unaware of the individual seller security levels since there is information asymmetry and only knows the average security level. This works to Seller 1's advantage.

In Variant 1.1, we modified the damage parameters to:

$$D_1 = 5, \quad D_2 = 7,$$

reducing those in Example 1 by a factor of 10, while keeping the remainder of the data as in Example 1. With lower associated financial damages in the case of a possible cyber attack, the sellers now substantially reduce their security levels with an increase in expected profits, although not significant.

In Variant 1.2, we kept the data as in Example 1, but we increased the damage parameters by a factor of 4 to:

$$D_1 = 200, \quad D_2 = 280.$$

With large damages for both sellers, in the case of a cyber attack, the sellers increase their security levels with a decrease in expected profits due to the increased costs.

In Variant 1.3, we used the data for Example 1 but we modified the demand price function to:

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

Hence, the buyer is now more sensitive to the average security level. The sellers, in order to satisfy the buyer, increase their security levels, as compared to those in Example 1. The buyer responds with an increased demand for the product and the sellers increase their expected profits since the buyer is willing to pay a higher price for the product due to enhanced average security.

In Variant 1.4, we, again, increase the sensitivity of the buyer to the average security level, so that now the demand price function is

$$\rho_1(d, \bar{s}) = -d_1 + 10(\frac{s_1 + s_2}{2}) + 100$$

with the remainder of the data as in Example 1. With even greater sensitivity of the buyer to average network security, both sellers respond with increased security levels, the highest of all examples in this set. Each seller also increases his product transaction volume and the price for the product increases by almost 10%. The expected profit for each seller increases substantially.

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	24.26	24.27	24.49	26.70
Q_{21}^*	21.27	21.28	21.27	21.49	23.70
d_1^*	45.54	45.54	45.54	45.98	50.40
s_1^*	.95	.81	.98	.96	.98
s_2^*	.96	.84	.99	.97	.98
$\bar{s}^*$	.955	.83	.985	.965	.98
$\rho_1(d_1^*, \bar{s}^*)$	54.55	54.54	54.55	54.98	59.40
$E(U_1)$	882.35	883.00	881.12	898.52	1069.37
$E(U_2)$	677.12	678.42	675.72	691.26	842.10

In Figure 3, we display the expected profits at equilibrium of the two sellers as the demand price coefficient for average security of Buyer 1 varies in Example 1. Figure 3 depicts graphically the expected profits obtained in Example 1, and its Variants 1.3 and 1.4, with the addition of the result for the demand price average security level coefficient being equal to 5. As can be seen from Figure 3, both sellers benefit financially as the buyer values the average security more highly. Such information is of use to sellers, since, as a buyer values average security higher, this leads to higher expected profits for the sellers. This sensitivity analysis demonstrates that a buyer can act as a positive driver for enhanced cybersecurity investments of sellers, even under information asymmetry. Hence, sellers may wish to seek out such buyers.

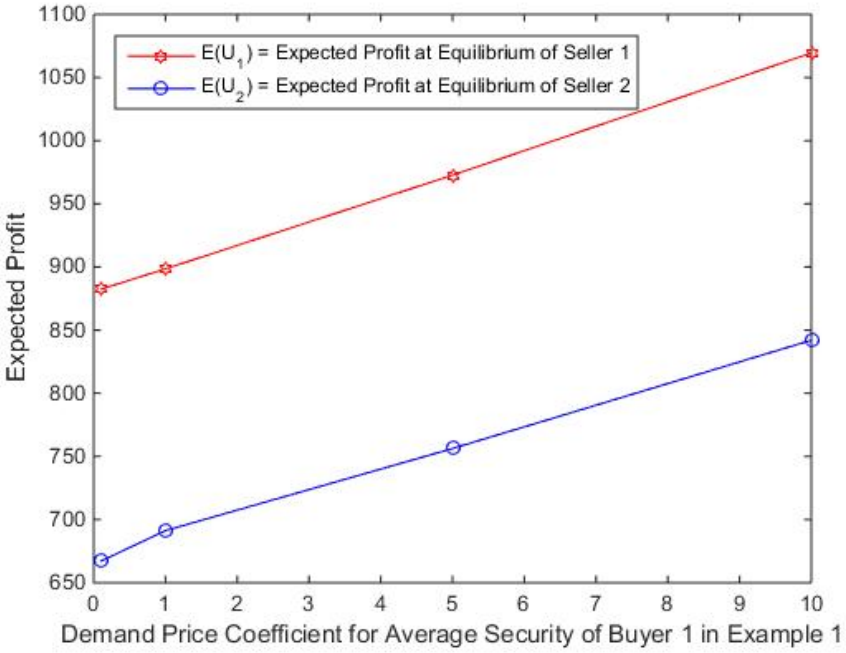

Figure 3: Sensitivity Analysis for Demand Price Coefficient for Average Security of Buyer 1 in Example 1

Example Set 2

The second set of examples has the network topology depicted in Figure 4. Specifically, we added a second buyer. The equilibrium solutions for this set of examples are reported in Table 2. Sensitivity analysis results for changes in cybersecurity investment cost functions are then given in graphical form in Figures 5 and 6.

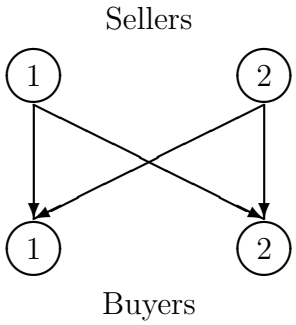

Figure 4: Network Topology for Example Set 2

Example 2, which is the baseline for this set, is constructed from Example 1 above but with the following data added for Buyer 2.

The new cost and demand price functions are:

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

$$\rho_2(d_2, \bar{s}) = -.5d_2 + .2(\frac{s_1 + s_2}{2}) + 200.$$

It is interesting to compare the solution of Example 2 with that of Example 1. Observe that, with the addition of a new buyer, which is more sensitive to average security, both sellers increase their security levels. The addition of a new buyer also increases the expected profits for both sellers just under tenfold for the first seller and over tenfold for the second seller.

In the first variant of Example 2, Variant 2.1, we modify the demand price function of Buyer 1 to reflect, for example, an increased willingness to pay more for the product because of its value. The new demand price function of Buyer 1 is now:

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

The product transactions to Buyer 1 more than double from their respective values in Example 2. The security levels remain unchanged. Both sellers benefit from increased expected profits.

Variant 2.2 in this set is constructed from Variant 2.1. We assume now that Buyer 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 2.1. The product transactions decrease by an order of magnitude to the second buyer and the sellers suffer from much decreased expected profits as compared to those in Variant 2.1 of this set of examples.

Variant 2.3 in this set is constructed from Example 2 to investigate the impacts of an increase in both the security investment functions so that:

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

with new damages: $D_1 = 500$ and $D_2 = 700$. With the increased costs associated with cybersecurity investments both sellers reduce their security levels to the lowest level of all the examples solved to this point.

Variant 2.4 in this set had the same data as Variant 2.3, but we now even further increase Seller 2's investment cost function where:

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

This could reflect, for example, a scenario where Seller 2 has expanded his cyber infrastructure and needs to invest more in appropriate software to protect the network. Seller 2 now has an equilibrium security level that is one quarter of that in Variant 2.3. Interestingly, not only do his expected profits decline but also those of Seller 1 do.

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}^*	24.27	49.27	49.27	24.27	24.26
Q_{12}^*	98.35	98.35	8.35	98.32	98.30
Q_{21}^*	21.27	46.27	46.27	21.27	21.26
Q_{22}^*	93.35	93.35	3.35	93.32	93.30
d_1^*	45.55	95.55	95.55	45.53	45.53
d_2^*	191.69	191.69	11.69	191.63	191.60
s_1^*	.96	.96	.96	.79	.79
s_2^*	.97	.97	.96	.83	.21
$\bar{s}^*$	.965	.965	.96	.81	.50
$\rho_1(d_1^*, \bar{s}^*)$	54.55	104.55	104.55	54.55	54.53
$\rho_2(d_2^*, \bar{s}^*)$	104.35	104.35	104.35	104.35	104.30
$E(U_1)$	8136.68	10894.79	3692.71	8083.88	8077.98
$E(U_2)$	7212.55	9745.65	3218.61	7151.75	6763.43

In Figure 5, we display the sensitivity analysis results for the changes in equilibrium average security levels of the two sellers as the α_2 coefficient in Seller 2's investment function h_2 increases from 1 (Example 2) to 100 (Variant 2.3), to 1,000 (Variant 2.4), and, finally, to 2,000 and 3,000 (results not in Table 2). We see, from Figure 5, that at $\alpha_2 = 2,000$ the cost of investing in cybersecurity is sufficiently high enough that Seller 2 does not invest at all in cybersecurity.

In Figure 6, we display the expected profits at equilibrium of the two sellers at the same values of the α_2 as in Figure 5. The expected profit of Seller 2 drops precipitously whereas that of Seller 1 remains essentially level. Hence, Seller 1 bears the burden of cybersecurity investments once Seller 2's investment function parameter α_2 reaches 2,000. This sensitivity analysis focuses on the "supply" side in terms of cybersecurity investment costs, as opposed to the "demand" side in terms of price function changes as done for the previous Example

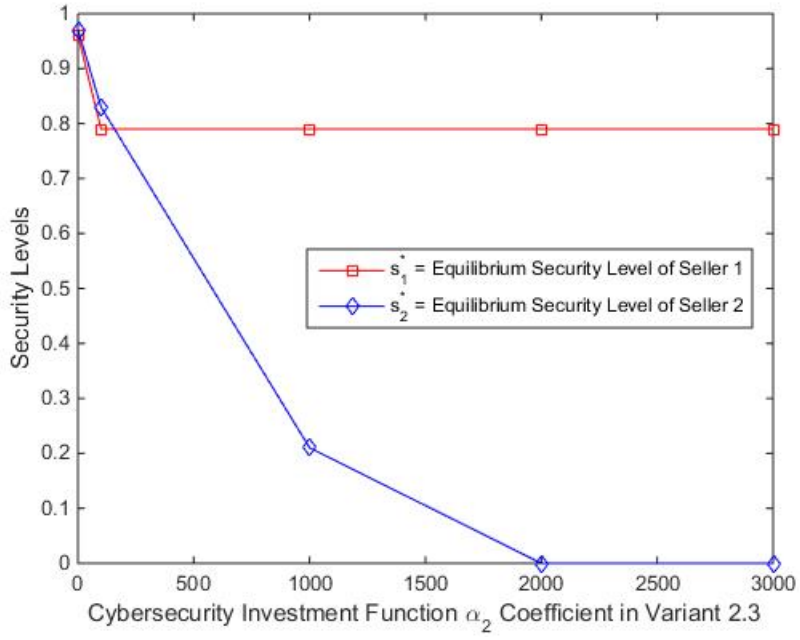

Figure 5: Sensitivity Analysis for Cybersecurity Investment Function α_2 Coefficient in Variant 2.3

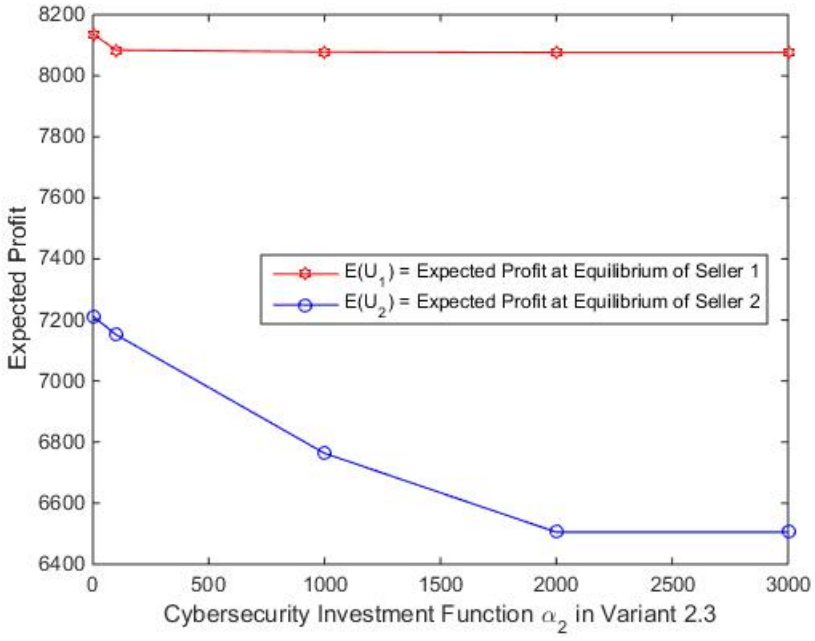

Figure 6: Sensitivity Analysis for Cybersecurity Investment Function α_2 Coefficient in Variant 2.3

1 sensitivity analysis. This analysis is useful to third parties, such as insurance companies, who can see the impact of higher cybersecurity investment costs on security levels, with the

security investments even dropping down to zero. In this case, Seller 2, who does not invest at all in cybersecurity, is at greater risk associated with cyber attacks, unlike Seller 1, who has invested in security.

Example Set 3

The third set of numerical examples consists of three sellers and two buyers. as depicted in Figure 7 with the subsequent sensitivity analysis results evaluating the impact of additional sellers reported in Figures 8 through 10.

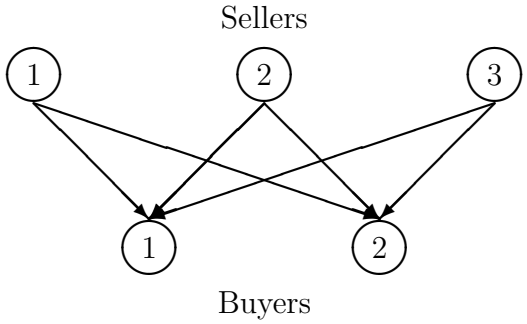

Figure 7: Network Topology for Example Set 3

In order to do cross comparisons among the different example sets, we construct Example 3, which is the baseline example in this set, from Example 2 in Set 2. Hence, the data for Example 3 is identical to that in Example 2 except the new Seller 3 data are as given below:

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

$$h_3(s_3) = 2(\frac{1}{\sqrt{(1-s_3)}} - 1), \quad D_3 = 100.$$

Also, since there are now 3 sellers, 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 3 are reported in Table 3. With increased competition, due to the addition of Seller 3, the demand prices for the product drop for both Buyer 1 and Buyer 2 (as compared to the respective equilibrium prices for Example 2). Also, with the increased competition, the expected profits drop for the two original sellers. The demand increases at Buyer 1 and also for Buyer 2, both at upwards of 10%.

Variant 3.1 in Set 3 is constructed from Example 3 with the data as therein except for the demand price function for Buyer 1 who now is more sensitive to the average security,

Table 3: Equilibrium Solutions for Examples in Set 3

Solution	Ex. 3	Var. 3.1	Var. 3.2	Var. 3.3	Var. 3.4
Q_{11}^*	20.81	21.00	21.00	11.64	12.68
Q_{12}^*	89.50	89.50	89.85	49.66	51.86
Q_{21}^*	17.81	17.99	17.99	9.64	10.68
Q_{22}^*	84.50	84.50	84.85	46.32	48.53
Q_{31}^*	13.87	13.99	14.00	8.73	9.51
Q_{32}^*	35.40	35.40	35.54	24.50	25.60
d_1^*	52.48	52.98	52.98	30.02	32.87
d_2^*	209.39	209.39	210.23	120.48	125.99
s_1^*	.96	.96	.97	.96	.99
s_2^*	.97	.97	.97	.97	.99
s_3^*	.95	.96	.96	.96	.97
$\bar{s}^*$	.96	.961	.966	.963	.981
$\rho_1(d_1^*, \bar{s}^*)$	47.61	47.98	47.99	40.93	44.06
$\rho_2(d_2^*, \bar{s}^*)$	95.50	95.50	95.85	80.49	83.82
$E(U_1)$	6655.25	6667.06	6714.85	3420.18	3765.72
$E(U_2)$	5828.73	5838.82	5883.93	2913.47	3230.19
$E(U_3)$	2261.46	2268.47	2283.75	1426.07	1581.55

where

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

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

Variant 3.2 in this set is constructed from Variant 3.1 with the only change being that now Buyer 2 is also more sensitive to average security so that his demand price function is:

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

We see, from Table 3, that the expected profits are now even higher than for Variant 3.1. These two variants demonstrate that consumers who care about security can enhance the expected profits of sellers of a product, further reinforcing the results obtained for Example Set 2.

Note that Seller 2 has not increased his security level in Variant 3.1 and Variant 3.2 as compared to that in Example 3, whereas Seller 1 and Seller 3 have. Hence, Seller 2, here, benefits from the information asymmetry.

Variant 3.3 in this set has the same data as Variant 3.2 except that the demand 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 3, the product transactions have all decreased substantially, as compared to the respective values for Variant 3.2 in this set of examples. Also, the demand prices associated with the two buyers have decreased substantially as have the expected profits for all the sellers.

Variant 3.4 in this set is constructed from Variant 3.3 except that now the demand price function sensitivity for both buyers has increased even more so that:

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

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

We then proceeded to conduct the following sensitivity analysis. To Variant 3.4 we added a fourth seller with the identical data to that of Seller 3 and then a fifth seller, also with identical data to that of Seller 3. The demand price functions were then modified accordingly to include the corresponding average security level.

In Figure 8, we display the equilibrium demands and the incurred equilibrium demand prices and in Figure 9 the average security levels at equilibrium. With increasing competition, the demand prices decrease and the demand increases for both Buyer 1 and Buyer 2. As can be seen from Figure 9, the average equilibrium security levels decrease. This may be due, in part, to sellers being less likely to be recognized (and suffer the consequences) for lower cybersecurity investments and, hence, they invest less.

In Figure 10, we display the impact on the sellers' expected profits as the number of sellers increases from 3 to 4 to 5, with again, Sellers 4 and 5 being identical to Seller 3. Sellers 4 and 5 have the same expected profits as does Seller 3 since they are identical. Figure 10 clearly reveals that increasing competition has a negative effect on all the sellers. Buyers, on the other hand, benefit from reduced prices.

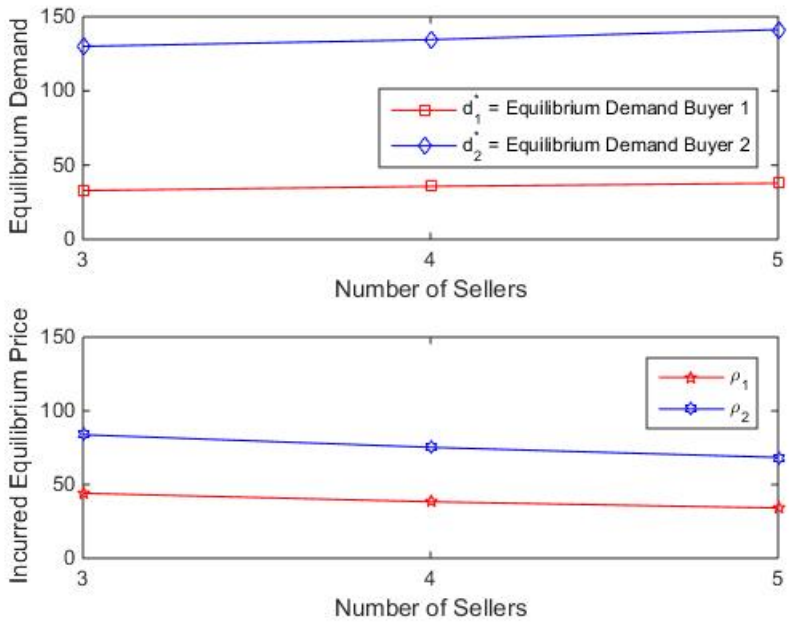

Figure 8: Sensitivity Analysis for an Increase of Sellers - Impacts on Equilibrium Demands and Incurred Demand Prices

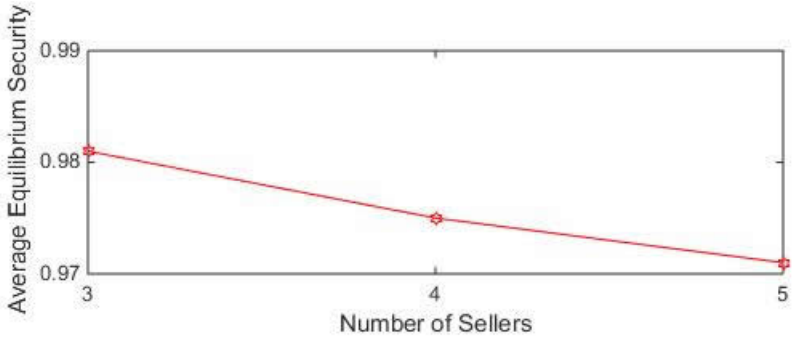

Figure 9: Sensitivity Analysis for an Increase of Sellers - Impact on Average Equilibrium Security

5. Summary

Cyber attacks have impacted businesses and other organizations as well as governments and individuals. Such attacks may result in financial losses as well as reputational costs, not to mention inconvenience and disruptions. Investments in cybersecurity are a mechanism in which to reduce financial damages in the case of a cyberattack.

In today's networked marketplaces buyers can purchase products in brick and mortar establishments or online; the same for many financial product transactions. Hence, they are also sensitive to the cybersecurity provided by the sellers, as recent cyber attacks of major

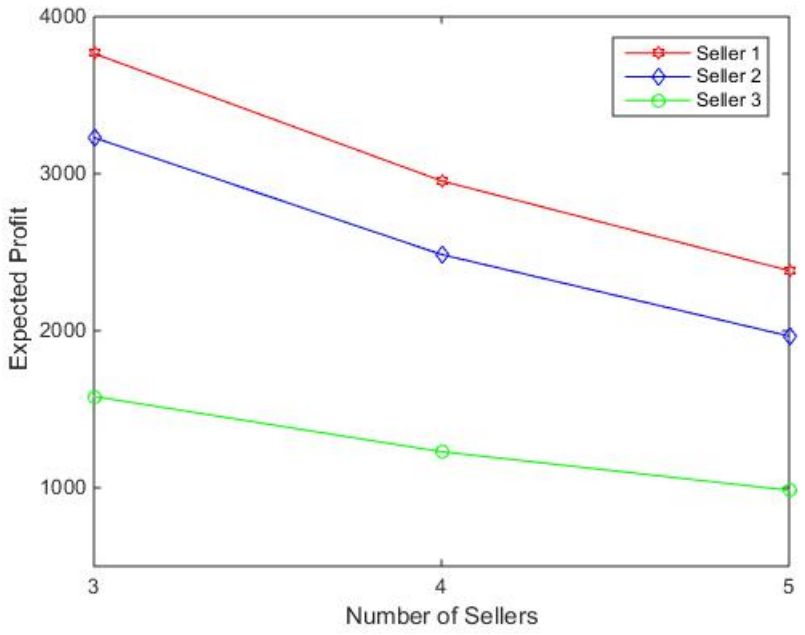

Figure 10: Sensitivity Analysis for an Increase of Sellers - Impact on Expected Profits

retailers have demonstrated. To tackle the challenges posed by cyber attacks and cybercrime there has been growing interest in developing methodological tools that can assist decision-makers in their cybersecurity investments. It is important to note that buyers interact with multiple sellers through the prices that they are willing to pay for the product. The prices depend on the quantities provided by the sellers of the product as well as the average security level for the marketplace.

In this paper, we develop a game theory model whose solution provides the equilibrium product transactions between sellers and buyers as well as the security levels of the sellers in the case of security information asymmetry. It is reasonable to expect that buyers may be aware of an industry average in terms of cybersecurity levels (and associated investments) but unlikely that they would know an individual seller's security levels. We construct probabilities from the security levels of the sellers, identify the expected financial damages, in the case of a cyber attack, and reveal the expected profit functions of the sellers. The sellers compete non-cooperatively, each one maximizing his expected profit until a Nash equilibrium is achieved. We derive the variational inequality formulation of the governing equilibrium conditions, and establish existence and uniqueness results for the equilibrium product transaction and security level pattern. From our model, once solved, the sellers can identify how much to invest in cybersecurity so as to maximize their expected profits, given the cybersecurity investments of their competitors. The model can be applied, as desired,

in different application settings and would require parameterization and obtaining data in terms of costs (processing, transaction, and cybersecurity investment ones), damages due to a cyberattack (type under consideration) as well as price function data for the product that the sellers provide. The latter would include not only dependencies on the demands but also on the average security level sensitivity, which, clearly, would depend on the buyer. Such data could be acquired, for example, from surveys or from specific industry reports. Furthermore, should governmental regulations be imposed as to the reporting of security levels, then this would provide another source of data.

The proposed computational scheme has nice features for implementation and results in closed form expressions, at each iteration, for the product transactions and security levels. The algorithm is then applied to compute solutions to three sets of increasingly more complex numerical examples (with a total of fifteen examples) in which we explore the addition of buyers and sellers, as well as the impacts of changes in the investment cost functions and the demand price functions on the equilibrium pattern. We also, include, after each example set, additional results, in the form of sensitivity analysis, and, for the final set, we report the impacts of the addition of identical sellers on the equilibrium demands, the incurred equilibrium demand prices, the average equilibrium security, and the expected profits of the sellers.

Future research may include the investigation of additional interdependencies in the buyer-seller network in terms of security, the development of cybersecurity investment models with product differentiation in that buyers are aware of the security levels of individual sellers, the construction of appropriate insurance schemes, and the study of the impacts of the imposition of minimum security levels.

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 three anonymous reviewers and the Editor for constructive comments and suggestions on two earlier versions of this paper.

References

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

[2] Alter, D. (2014). Security investent more important than ever after latest data breaches. Money Morning, September 8.

[3] Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314 (5799), 610-613.

[4] Cavasoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. Journal of Management Information Systems, 25(2), 281-304.

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

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

[7] Dafermos S., & Nagurney, A. (1987). Oligopolistic and competitive behavior of spatially separated markets. Regional Science and Urban Economics, 17, 245-254.

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

[9] Gabay, D., & Moulin, H. (1980). 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, 271-294.

[10] Gartner (2013). Gartner reveals top 10 security myths, by Ellen Messmer, NetworkWorld, June 11, 2013.

[11] Gordon, L.A., & Loeb, M.P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457.

[12] Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. Information Systems Frontiers, 8(5), 338-349.

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

[14] Kunreuther, H., & Heal, G. (2003). Interdependent security. The Journal of Risk and Uncertainty 26 (2/3), 231-249.

[15] Manshei, M.H., Alpcan, T., Basar, T., & Hubaux, J.-P. (2013). Game theory meets networks security and privacy. ACM Computing Surveys, 45(3), 25:1-25:34, June.

[16] Market Research (2013). United States Information Technology report Q2 2012, April 24.

[17] Matsuura, K. (2008). Productivity space of information security in an extension of the Gordon-Loeb's investment model. Proceedings of the Seventh Workshop on the Economics of Information Security (WEIS2008), Tuck School of Business, Dartmouth College, Hanover, New Hampshire, June 25-28.

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

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

[20] Nagurney, A., & Li, D. (2014). Equilibria and dynamics of supply chain network competition with information asymmetry in quality and minimum quality standards. Computational Management Science, 11(3), 285-315.

[21] Nagurney, A., Li, D., Wolf, T., & Saberi, S. (2013). A network economic game theory model of a service-oriented Internet with choices and quality competition. Netnomics, 14(1-2), 1-25.

[22] Nagurney, A., & Yu, M. (2012). Sustainable fashion supply chain management under oligopolistic competition and brand differentiation. International Journal of Production Economics, 135, 532-540.

[23] Nagurney, A., Yu, M., & Qiang, Q. (2011). Supply chain network design for critical needs with outsourcing. Papers in Regional Science, 90, 123-142.

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

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

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

[27] Ponemon Institute (2013). Second annual cost of cyber crime study: Benchmark study of U.S. companies.

[28] PriceWaterhouseCoopers (2014). Global economic crime survey.

[29] 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.

[30] 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.

[31] Tatsumi, K., & Goto, M. (2009). Optimal timing of information security investment: A real options approach. In Proceedings of the the Eighth Workshop on the Economics of Information Security (WEIS 2009), University College London, England, June 24-25.

[32] Varian, H.R. (2004). System reliability and free riding. In: Camp, L.J., Lewis, S. (Ed.), Economics of information security. Boston, Massachusetts: Kluwer Academic Publishers, 1-15.

[33] Zhang, D., & Nagurney, A. (1995). On the stability of projected dynamical systems. Journal of Optimization Theory and its Applications, 85, 97-124.