Multifirm Models of Cybersecurity Investment Competition vs. Cooperation and Network Vulnerability

Anna Nagurney and Shivani Shukla
Department of Operations and Information Management
Isenberg School of Management
University of Massachusetts, Amherst, Massachusetts 01003

April 2016; revised August 2016; revised October 2016

European Journal of Operational Research (2017), **260(2)**, pp 588-600.

Abstract:

In this paper, we develop and compare three distinct models for cybersecurity investment in competitive and cooperative situations to safeguard against potential and ongoing threats. We introduce a Nash equilibrium model of noncooperation in terms of cybersecurity levels of the firms involved, which is formulated, analyzed, and solved using variational inequality theory. The equilibrium of this model then acts as the disagreement point over which bargaining takes place in the setting of the second model, which yields a cooperative solution in which the firms are guaranteed that their expected utilities are no lower than those achieved under noncooperation. Nash bargaining theory is utilized to argue for information sharing and to quantify its monetary and security benefits in terms of reduction in network vulnerability to cyberattacks. The third model in this paper also focuses on cooperation among the firms in terms of their cybersecurity levels, but from a system-optimization perspective in which the sum of the expected utilities is maximized. Qualitative properties are provided for the models in terms of existence and uniqueness results along with numerical solutions to two cases focusing on retailers and financial service firms, since these have been subject to some of the most damaging cyberattacks. Sensitivity analysis results are also provided. We compare the solutions of the models for the cases and recommend a course of action that has both financial and policy-related implications.

Key words: cybersecurity, investments, game theory, Nash equilibrium, Nash bargaining, system-optimization, network vulnerability, variational inequalities, retailers, financial services

1. Introduction

The effects of cyberattacks are being felt across the globe in multiple sectors and industries. The damages incurred include direct financial damages as well as reputation issues, the loss of business, the inability to provide the expected services, opportunity costs, and the loss of trust. According to the Center for Strategic and International Studies (2014), the world economy sustained $445 billion in losses from cyberattacks in 2014. The United States suffered a loss of $100 billion, Germany lost $60 billion, China lost $45 billion, and the United Kingdom reported a loss of $11.4 billion due to cybersecurity lapses. The think tank also presented an analysis that indicated that of the $2 trillion to $3 trillion generated by the Internet annually, about 15%-20% is extracted by cybercrime. Adversaries in the cyber realm include spies from nation-states who seek our secrets and intellectual property; organized criminals who want to steal our identities and money; terrorists who aspire to attack our power grid, water supply, or other infrastructure; and hacktivist groups who are trying to make a political or social statement (Deloitte (2014)).

The evolving threat landscape of cybercrime heavily targets organizations in energy, retail, financial services, critical manufacturing, communications, and even healthcare. According to the US Department of Homeland Security (2015), the energy sector constituted the highest number of incidents (32%) reported in Fiscal Year 2014. The reality of effects of cyberattacks on energy infrastructure is brought forth by the recent “UglyGorilla” attack in 2014 that sought access to pipeline schematics and natural gas flow regulations systems in the United States through the remote shutdown of critical systems (Bloomberg (2014)). In order to protect the electric grids, and oil and natural gas infrastructure from threats, the Energy Department in October 2015 announced $34 million toward R&D efforts (US Department of Energy (2015)). The retail sector, on the other hand, has reported to-date one of the biggest breaches with heavy losses. In 2014 alone, Target, Home Depot, Michaels Stores, Staples, and eBay were breached. Card data and personal information of millions of customers were stolen and the detection of cyber espionage became the prime focus for the retail sector with regards to cybersecurity (Granville (2015)). Since financial gains, through the subversion of processes and controls, are one of the most attractive benefits emerging from cyberattacks, financial service firms are targeted incessantly. The large-scale data breach of JP Morgan Chase, Kaspersky Lab’s detection of a two-year infiltration of 100 banks across the world costing $1 billion (USA Today (2015)), and the Dridex malware related losses of $100 million worldwide (Dodd (2015)) are some of the widely accepted cautionary tales in this sector.

According to the Ponemon Institute (2015), the average annualized cost of cybercrime incurred by a benchmark sample of organizations was $15 million. The range of these annualized costs was \$1.9 million to \$65 million, an 82% increase in the past six years. Most of these cybercrimes are generally caused by denial of service, malicious insiders, and malicious code affecting physical and cyber assets. A survey conducted by AON Risk Services with Ponemon Institute (2015) concluded that despite the comparability of the average potential loss to information assets (\$617 million) and property, plant and equipment (\$648 million), the percentages of insurance coverage are 51% and 12%, respectively. Moreover, because of the interlinkages among different firms, organizations, institutions, and even nations, due to the Internet and associated advanced technologies, a single firm, organization, nation, or even individual may affect the vulnerability of others to cyberattacks. The technological innovations that are being envisioned could intensify these losses even more as they introduce new entry points for cyberattacks (The Wall Street Journal (2014)). These inclement costs ultimately trickle down to organizations and consumers.

For example, the Internet of Things (IoT) has expanded the possible entry points for cyberattacks (ComputerWeekly.com (2015)). According to McKinsey & Company Quarterly (2014), worries about cyberattacks are beginning to have quantifiable negative business implications. In high tech, half of the McKinsey executives surveyed said they would modify the characteristics of their R&D efforts over time with added concerns that cyberattacks could slow down the capture of value creation from cloud computing, mobile technologies, and healthcare technologies. As reported therein, 70% of the respondents noted that security concerns had delayed the adoption of public cloud computing by a year or more, and 40% said that because of such concerns enterprise-mobility capabilities were delayed by a year or more.

The increased rate of cyberattacks has spurred the behavioral analysis of attackers and defenders. Aggarwal et. al. (2015) take a game theory approach to study actions of attackers and defenders in a 2 × 4 cybersecurity game that is evaluated computationally through 1000 simulations. A defense exercise model using game theory is developed by Patrascu and Simion (2014) to train cyber response specialists. Nagurney (2015) utilized a network economics approach to model cybercrime emphasizing that both firms and hackers act as economic agents. RAND National Security Division (2014) also argued that an economic approach to tackling cybercrime is warranted.

In addition to investigating interactions among attackers and defenders, there has also been a growing literature on cybersecurity investments. The investment in cybersecurity through software and hardware, education, and effective personnel can help resist the growing frequency and severity of attacks, and assist in the planning of appropriate allocation of resources required to prevent/mitigate the likely damage. Garvey, Moynihan, and Servi

(2013) suggested an approach that helps to prioritize among competing investment options for better cyber defense. They identify sets of Pareto efficient cost-benefit investments, and their economic returns, that capture tangible and intangible advantages of countermeasures that strengthen cybersecurity. From a social welfare standpoint, Gordon et. al. (2015) examined changes in the maximum a firm should invest into cybersecurity activities in the face of well-recognized externalities.

Nevertheless, the domain of security in computer networks has a limited but useful literature employing game theory. Zero-sum, non-zero-sum, dynamic, stochastic, repeated, Stackelberg, static, and coalition games have been applied to computer and communication networks. Manshaei et al. (2011) provide a survey of the literature combining game theory and security. The survey is divided into six main categories: security of the physical and MAC layers, security of self-organizing networks, intrusion detection systems, anonymity, and privacy, the economics of network security, and cryptography. Das (2015) presents a cybersecurity ecosystem consisting of network, cloud, and software providers and economically analyzes the risk of correlation between agents in the ecosystem in case of a breach. Shetty et al. (2009) and Shetty (2010) focus on game theory for the determination of cybersecurity levels through investments. In both those publications, the authors determine the Nash equilibrium as well as the social optimum associated with security levels. However, it is assumed that the firms face identical cybersecurity investment cost functions, have identical wealth, and also the damages afflicted due to a cyberattack are the same. Nagurney and Nagurney (2015) and Nagurney, Nagurney, and Shukla (2015), inspired, in part, by that research, relaxed the assumptions of identical firms, and further quantify the expected utilities of financial firms/retailers in a bipartite network with investment costs, supply prices, transaction costs, and demand price functions, taking a supply chain perspective. A variational inequality and noncooperative game theoretic approach is utilized to arrive at the equilibrium production quantities and cybersecurity levels given firm and consumer behavior that ultimately ascertain the network vulnerability. A recent edited volume by Daras and Rassias (2015) includes additional information on network security models and frameworks.

Nagurney (2015) emphasized the importance of assessing the vulnerabilities of cyberattacks in a rigorous quantifiable manner and identifying possible synergies associated with information sharing for firms providing critical infrastructure networks on which our economy and society depend. The complexity and interdependence of firms, governments, and individuals in intricately woven networks mean that an attack on one may pave the way for attacks on others. Given that the number and intensity of cyber threats for every industrial and non-industrial sector have increased, firms and governments are progressing toward sharing threat information to arrange coordinated defenses against attacks.

An increasingly connected world may amplify the effects of a disruption. Information Technology (IT) outages of any kind can lead to material losses as well as loss of data, unplanned downtime, and adverse impacts on the reputations of the affected organizations. Firms interacting with one another may be at varied levels of IT and security maturity. Cybersecurity related measures are found mostly at an organizational level. Breaking down these silos and sharing information can have a direct impact on business continuity. This makes security governance an integral part of risk management and business continuity strategies of organizations in the support of their client processes. We suggest that, by taking a network perspective, in evaluating both noncooperative and cooperative behavior in terms of cybersecurity investments, can provide insight into the value of information sharing. Nevertheless, information sharing may have its disincentives since cooperation on the cyber front is being struck between competitors in the market.

In this paper, we present three new models of cybersecurity investments. Our proposed models are not restricted to the number of firms, their locations, or the sectors that they belong to. We begin with a Nash equilibrium model of noncooperation and competition, which is formulated, analyzed, and solved using variational inequality theory. The solution to this Nash equilibrium model then serves as the disagreement point over which the bargaining takes place in the second model, which is one of cooperation. For this model, we utilize Nash bargaining theory, a type of cooperative game theory, to argue for the sharing of information on firms' security levels, where here security refers to cybersecurity. We assume that firms bargain with each other to decide upon the security levels that they would be willing to implement vis-a-vis their investment cost functions, wealth, and damages in the case of a cyberattack. The constraints guarantee that the expected utility of each firm is no lower than that obtained under the Nash equilibrium solution.

Nash bargaining theory was proposed in Nash (1950b). Considerable contributions to the area were made by Harsanyi (1977), who extended the original two-person game into a multi-player game and derived important theoretical deductions, and by Muthoo (1999), who applied the theory to various bargaining situations and demonstrated the usefulness. Various extensions of the theory and application to supply chains were proposed by Nagarajan and Sosic (2006). Boonen (2016) discusses strategic interaction between two firms that trade risk over the counter in a one period model, wherein the focus is on an incomplete set of risk redistributions. In the context of cybercrime, one of the extensions was employed by Wagner et al. (2012), who used Nash bargaining for resource allocation in cloud computing for collaborative defense. An optimization formulation of a collusive cooperative game with product quantities as variables was developed and solved as a nonlinear programming problem in Harrington et al. (2005). Jiang et al. (2009), later, analyzed cooperative content distribution and traffic engineering in ISP networks. Finally, Bakshi and Kleindorfer (2009) did not discuss cybersecurity, yet demonstrated the use of Nash bargaining and cooperative game theory towards investment for resilience in global supply chains. The paper utilized an axiomatic approach to bargaining.

The third model in this paper also focuses on cooperation among the firms in terms of their cybersecurity levels, but from a system-optimization perspective in which the sum of the expected utilities of all the firms is maximized. System-optimization models, but different from the one proposed here, were also developed for cybersecurity investments by Shetty et al. (2009) and Shetty (2010).

In addition to the model developments and the associated theory, here we also apply and compare the obtained solutions in terms of firm and network vulnerability. Moreover, we demonstrate the benefits of bargaining through case studies in the retail and financial services sectors.

The paper is organized as follows. In Section 2 we present the three distinct models, along with their qualitative properties. We also outline the algorithm for the determination of solutions to the noncooperative cybersecurity investment model governed by the Nash equilibrium, along with convergence results. In Section 3, we highlight the software utilized to compute solutions to the two cooperative cybersecurity investment models since these are highly nonlinear programming problems. We then provide solutions to the three distinct cybersecurity investment models for a spectrum of case studies in the retail and financial services sectors. We also provide sensitivity analysis results. The paper is summarized and the conclusions presented in Section 4.

2. The Multifirm Cybersecurity Investment Models

In this Section, we present three distinct multifirm cybersecurity investment models reflecting three distinct behavioral concepts. In the first model, the firms compete noncooperatively on their cybersecurity levels, each one trying to maximize its expected utility, with the governing concept being the Nash equilibrium (NE). In the second model, the firms cooperate under the Nash bargaining (NB) concept. The objective function therein, which is maximized, is the product over all the firms of each firm's expected utility minus its expected utility evaluated at the Nash equilibrium solution. The Nash equilibrium solution is here the disagreement point. The constraints guarantee that the firms' respective expected utilities are never less than those under the Nash equilibrium solution. In the third model, the solution concept is that of system-optimization (S-O), where the sum of the expected utilities of all the firms with respect to their cybersecurity investments is maximized. In each of the three models, the firms are also faced with bounds on the cybersecurity levels.

We first outline the common features of the models and in subsequent subsections we detail their specifics. The models are one period models, as in Kunreuther and Heal (2003), and, hence, the probability of an attack is defined over the period under study.

We assume that there are m firms in the "network." These firms can be financial service firms, energy firms, manufacturing firms, or even retailers. The network aspect lies in their connectivity in cyberspace through the Internet and in their frequent such interactions because of a common industry. We assume that each firm i; $i = 1, \dots, m$, in the network is interested in determining how much it should invest in cybsecurity with the cybersecurity level or, simply, security level of firm i denoted by s_i; $i = 1 \dots, m$.

The cybersecurity level s_i of each firm i must satisfy the following constraint:

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

where u_{s_i}<1, and is also greater than zero, is the upper bound on the security level for firm i. Note that a value of a cybersecurity level of 1 would imply perfect security, which is not achievable. When $s_i = 0$ the firm has no security. We group the security levels of all firms into the m-dimensional vector s.

In order to attain security level s_i, firm i encumbers an investment cost $h_i(s_i)$ with the function assumed to be continuously differentiable and convex. As noted in Shetty et al. (2009), the intuition is that user security costs increase with security, and that improving security level imposes an increasing marginal cost on the user. Distinct firms, 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 firm i, $h_i(0) = 0$ denotes an entirely insecure firm and $h_i(1) = \infty$ is the investment cost associated with complete security for the firm, as in Shetty et al. (2009) and Shetty (2010). An example of a suitable $h_i(s_i)$ function that we use in this paper is

$$h_i(s_i) = \alpha_i(\frac{1}{\sqrt{(1-s_i)}} - 1) \tag{2}$$

with $\alpha_i > 0$. Such a function was utilized in Nagurney and Nagurney (2015), in Nagurney, Nagurney, and Shukla (2015), and in Nagurney, Daniele, and Shukla (2015). In the latter reference strict convexity of the cyberinvestment cost function (2) was established. According to the cybersecurity investment cost function in (2), and, as noted in Shetty et al. (2009), it becomes increasingly costly to improve the security level at a higher level of security.

The network security level, $\bar{s}$, is the average security, given by:

$$\bar{s} = \frac{1}{m}\sum_{j=1}^{m} s_j. \tag{3}$$

The vulnerability of firm i, $v_i = (1 - s_i)$ and the network vulnerability, $\bar{v} = (1 - \bar{s})$. Similar measures, but in a supply chain cybersecurity investment context, were used by Nagurney, Nagurney, and Shukla (2015). Therein, however, only competition and not cooperation was considered and the strategic variables included product quantities in addition to security levels.

In this paper, we study how the network security and the network vulnerability vary under the three different behavioral concepts.

Following Shetty (2010), probability p_i of a successful attack on firm i; $i = 1, \ldots, m$, is

$$p_i = (1 - s_i)(1 - \bar{s}), \quad i = 1, \ldots, m, \tag{4}$$

where $(1 - \bar{s})$ is the probability of an attack on the network and $(1 - s_i)$ is the probability of success of such an attack on firm i.

Each firm i; $i = 1, \ldots, m$, has a utility associated with its wealth W_i, denoted by $f_i(W_i)$, which is increasing, and is continuous and concave. The form of the $f_i(W_i)$ that we use in this paper is $\sqrt{W_i}$ (see Shetty et al. (2009)). Such a function is increasing, continuous, and concave, reflecting that a firm's wealth has a positive but decreasing marginal benefit. Also, a firm i is faced with damage D_i if there is a successful cyberattack on it.

Hence, the expected utility $E(U_i)$ of firm i; $i = 1, \ldots, m$, is given by the expression:

$$E(U_i) = (1 - p_i)f_i(W_i) + p_i(f_i(W_i - D_i)) - h_i(s_i). \tag{5}$$

Note that, according to (3), each firm i encumbers an investment cost associated with cybersecurity, which, of course, is equal to zero if the security level s_i is zero. We group the expected utilities of all firms into the m-dimensional vector $E(U)$. In view of (2), we may write $E(U_i) = E(U_i(s)), \forall i$.

We emphasize that, in previous papers that focused on cybersecurity investments solely as in Shetty et al. (2009) and Shetty (2010), it was assumed that the firms were identical in that their valuation of wealth was the same, the financial damage after a successful attack was the same, their investment cost functions were the same, and the upper bounds on the security levels of the firms were all identically equal to 1. In our framework, the firms differ in these aspects, which provides greater realism. For example, the firms can have different wealth, value their wealth distinctly, have different damage due to a cyberattack, given their existing cyber infrastructure, and also have distinct associated cyberinvestment cost functions. Moreover, different firms may have distinct upper bounds on their achievable security levels. Furthermore, in contrast to the models in Shetty (2010), here we do not assume that an individual firm has a negligible effect on the network security level (3) and takes that value as given.

2.1 The Nash Equilibrium Model of Cybersecurity Investments

In our first model, we assume that the m firms compete noncooperatively, each one trying to maximize its expected utility. We seek to determine a security level pattern $s^* \in K^1$, where $K^1 = \prod_{i=1}^m K_i^1$ and $K_i^1 \equiv \{s_i | 0 \leq s_i \leq u_{s_i}\}$, such that the firms will be in a state of equilibrium with respect to their cybersecurity levels as defined below. Note that K^1 is convex since it is a Cartesian product of the firms' feasible sets with each such set being convex since it corresponds to box-type constraints.

We now present the Nash (1950a, 1951) equilibrium definition that captures the decision-makers' competitive behavior in our model.

Definition 1: Nash Equilibrium in Cybersecurity Levels

A security level pattern $s^* \in K^1$ is said to constitute a cybersecurity level Nash equilibrium if for each firm $i; i = 1, \ldots, m$:

$$E(U_i(s_i^*, \hat{s}_i^*)) \geq E(U_i(s_i, \hat{s}_i^*)), \quad \forall s_i \in K_i^1, \tag{6}$$

where

$$\hat{s_i^*} \equiv (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_m^*). \tag{7}$$

According to (6), a cybersecurity Nash equilibrium is established if no firm can unilaterally improve upon its expected profits by selecting an alternative security level.

We now present the variational inequality formulation of the Nash equilibrium in security levels.

Theorem 1: Variational Inequality Formulation of Nash Equilibrium in Cybersecurity Levels

If for each firm i; $i = 1, \ldots, m$, the expected profit function $E(U_i(s))$ is continuously differentiable, and concave, and the feasible set K^1 is convex, we know that $s^* \in K^1$ is a Nash equilibrium in cybersecurity levels according to Definition 1 if and only if it satisfies the variational inequality

$$-\sum_{i=1}^{m} \frac{\partial E(U_i(s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0, \quad \forall s \in K^1, \tag{8}$$

or, equivalently, $s^* \in K^1$ is a Nash equilibrium security level pattern if and only if it satisfies the variational inequality

$$\sum_{i=1}^{m} \left[\frac{\partial h_i(s_i^*)}{\partial s_i} + [f_i(W_i) - f_i(W_i - D_i)] \left[\frac{1}{m} \sum_{j=1}^{m} s_j^* - 1 - \frac{1}{m} + \frac{s_i^*}{m} \right] \right] \times (s_i - s_i^*) \geq 0, \forall s \in K^1. \tag{9}$$

Proof: Since the feasible set is convex for each firm, and minus the expected utility, -$E(U_i(s))$, is convex, we know from the classical theory of variational inequalities (see also Gabay and Moulin (1980)), that each firm i; $i = 1, \ldots, m$, maximizes its expected utility if and only if

$$-\frac{\partial E(U_i(s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0, \quad \forall s_i \in K_i^1. \tag{10}$$

Summing the inequality (10) over all firms yields the variational inequality (8).

Variational inequality (9), in turn, is equivalent to variational inequality (8) with notice of (5) so that the expansion of

$$-\frac{\partial E(U_i(s^*))}{\partial s_i}$$

$$= \frac{\partial h_i(s_i^*)}{\partial s_i} + f_i(W_i) \left[\frac{1}{m} \sum_{j=1}^{m} s_j^* - 1 - \frac{1}{m} + \frac{s_i^*}{m} \right] + f_i(W_i - D_i) \left[1 - \frac{1}{m} \sum_{j=1}^{m} s_j^* + \frac{1}{m} - \frac{s_i^*}{m} \right]$$

$$= \frac{\partial h_i(s_i^*)}{\partial s_i} + [f_i(W_i) - f_i(W_i - D_i)] \left[\frac{1}{m} \sum_{j=1}^{m} s_j^* - 1 - \frac{1}{m} + \frac{s_i^*}{m} \right], \tag{11}$$

for each firm i. The conclusion follows. □

We now put variational inequality (9) into standard variational inequality form (see Nagurney (1999)), that is: determine $X^* \in \mathcal{K} \subset R^N$, such that

$$\langle F(X^*), X - X^* \rangle \geq 0, \quad \forall X \in \mathcal{K}, \tag{12}$$

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 m-dimensional vectors $X \equiv s$ and $F(X)$ with the i-th component, F_i, of $F(X)$ given by

$$F_i(X) \equiv -\frac{\partial E(U_i(s))}{\partial s_i}$$

$$= \frac{\partial h_i(s_i)}{\partial s_i} + [f_i(W_i) - f_i(W_i - D_i)] \left[\frac{1}{m} \sum_{j=1}^{m} s_j - 1 - \frac{1}{m} + \frac{s_i}{m} \right], \tag{13}$$

and with the feasible set $\mathcal{K} \equiv K^1$ and $N = m$. Then, clearly, variational inequality (8) and (9) can be put into standard form (12).

A solution to variational inequality (12) for our Nash equilibrium cybersecurity investment model is guaranteed to exist since the function $F(X)$ is continuous and the feasible set $\mathcal{K} = K^1$ is compact (see Kinderlehrer and Stampacchia (1980) and Nagurney (1999)). The uniqueness result also follows from the classical theory of variational inequalities.

Theorem 2: Uniqueness of the Nash Equilibrium

If $F(X)$ is strictly monotone, that is:

$$\langle (F(X^1) - F(X^2)), X^1 - X^2 \rangle > 0, \quad \forall X^1, X^2 \in \mathcal{K}, X^1 \neq X^2, \tag{14}$$

then X^*, the solution to variational inequality (12), is unique.

We now provide an interpretation of the strict monotonicity property directly for the Nash equilibrium model. Specifically, we know that if the Jacobian of $F(X)$, which we denote by J, is positive definite, then $F(X)$ is strictly monotone.

We construct:

$$\frac{\partial F_i}{\partial s_i} = \frac{3\alpha_i}{4(1 - s_i)^{2.5}} + \frac{2}{m}[f_i(W_i) - f_i(W_i - D_i)], \tag{15a}$$

and

$$\frac{\partial F_i}{\partial s_j} = \frac{1}{m}[f_i(W_i) - f_i(W_i - D_i)], \quad \text{for } j \neq i. \tag{15b}$$

It then follows that

$$J = \begin{bmatrix} \frac{3\alpha_1}{4(1-s_1)^{2.5}} + \frac{2}{m}[f_1(W_1) - f_1(W_1 - D_1)] & \cdots & \frac{1}{m}[f_1(W_1) - f_1(W_1 - D_1)] \\ \vdots & & \vdots \\ \frac{1}{m}[f_m(W_m) - f_m(W_m - D_m)] & \cdots & \frac{3\alpha_m}{4(1-s_m)^{2.5}} + \frac{2}{m}[f_m(W_m) - f_m(W_m - D_m)] \end{bmatrix},$$

We know that (see, e.g., Nagurney (1999)), if $(J+J^T)/2$, where J need not be symmetric, is strictly diagonally dominant, then it is positive definite and $F(X)$ is then strictly monotone. From the structure of $(J+J^T)/2$ we can infer that it is strictly diagonally dominant if

$$\frac{3\alpha_i}{4(1-s_i)^{2.5}} > \frac{m-5}{2m}[f_i(W_i) - f_i(W_i - D_i)] + \frac{1}{2m}\sum_{j=1;j\neq i}^{m}[f_j(W_j) - f_j(W_j - D_j)], \quad i = 1, \ldots, m. \tag{16}$$

One can deduce that (16) will be satisfied, for example, for $m = 3$, if $2[f_i(W_i) - f_i(W_i - D_i)] \geq \sum_{j=1}^{m}[f_j(W_j) - f_j(W_j - D_j)], j \neq i$. Analogous conditions can be determined for $m = 2$, and so on. Specifically, for $m = 2$ if the following condition is satisfied then strict diagonal dominance of $(J + J^T)/2$ also holds:

$$3(f_1(W_1) - f_1(W_1 - D_1)) \geq f_2(W_2) - f_2(W_2 - D_2) \geq \frac{f_1(W_1) - f_1(W_1 - D_1)}{3}. \tag{17}$$

This result is useful since we then have a unique disagreement point.

Of course, positive definiteness of J can still hold even when the strict diagonal dominance condition does not.

There are numerous algorithms that can be applied to compute the solution to (12). In this paper, we utilize the Euler method, detailed below for the numerical study in Section 3. Specifically, the statement of the Euler method, due to Dupuis and Nagurney (1993), is as follows. Iteration τ of the Euler method where the variational inequality is expressed in standard form (12) is:

$$X^{\tau+1} = P_{\mathcal{K}}(X^\tau - a_\tau F(X^\tau)), \tag{18}$$

where $P_{\mathcal{K}}$ is the projection on the feasible set $\mathcal{K}$ and F is the function that enters variational inequality (12) in which $X \equiv s$ and $F(X)$ consists of the components as defined in (9). As established in Dupuis and Nagurney (1993), for convergence of the general iterative scheme, which induces the Euler method, the sequence $\{a_\tau\}$ must satisfy: $\sum_{\tau=0}^{\infty} a_\tau = \infty$, $a_\tau > 0$, $a_\tau \to 0$, as $\tau \to \infty$. Also, assume that $F(X)$ is strictly monotone at some solution X^* to the variational inequality (12).

If, however, $F(X)$ is not strictly monotone, but only monotone, and Lipschitz continuous, the modified projection method of Korpelevich (1977) can be used. It is essential to note that, in the absence of strict monotonicity, there may be multiple Nash equilibria. If so, firms will prefer the equilibria that are Pareto optimal. For multiple such equilibria, there are Nash equilibrium solutions. Boonen (2016) studies regulators that aim to optimize welfare of firms while enforcing an attractive Pareto optimal solution by restricting the joint feasible space. Conditions for convergence of the Euler method for a variety of network-based problems can be found in Nagurney and Zhang (1996) and Nagurney (2006).

In view of the simple structure of the underlying feasible set, the Euler method yields at each iteration closed form expressions for the security levels: i; $i = 1, \ldots, m$, given by:

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

$$\max\{0, \min\{u_{s_i}, s_i^\tau + a_\tau(-\frac{\partial h_i(s_i^\tau)}{\partial s_i^\tau} - (f_i(W_i) - f_i(W_i - D_i))\left[\frac{1}{m}\sum_{j=1}^{m} s_j^\tau - 1 - \frac{1}{m} + \frac{s_i^\tau}{m}\right]\}\}. \quad (19)$$

The complete statement of the algorithm to implement for the solution of this model is given below:

Step 0: Initialization

Set $s^0 \in \mathcal{K}$. Let $\tau = 0$ and set the sequence $\{a_\tau\}$ so that $\{a_\tau\}$ satisfies: $\sum_{\tau=0}^{\infty} a_\tau = \infty$, $a_\tau > 0$, $a_\tau \rightarrow 0$, as $\tau \rightarrow \infty$.

Step 1: Computation

Compute $s_i^{\tau+1}$; $i = 1, \ldots, m$, according to (19).

Step 2: Convergence Verification

If max $|s_i^{\tau+1} - s_i^\tau| \leq \epsilon$, for all i, with $\epsilon > 0$, a prespecified tolerance, then stop; otherwise, set $\tau := \tau + 1$, and go to Step 1.

2.2 The Nash Bargaining Model of Cybersecurity Investments

The bargaining model proposed by Nash (1950b, 1953) is based on axioms and focused on two players, that is, decision-makers. The framework easily generalizes to m decision-makers, as noted in Leshem and Zehavi (2008). Here the decision-makers are firms. An excellent overview can be found in Binmore, Rubinstein, and Wolinsky (1989) and in the book by Muthoo (1999). In our Nash bargaining model, we use expected utilities, rather than utilities, since we are dealing with uncertainties as represented by the probabilities of cyberattacks.

Let $E(U_j^{NE})$ denote the expected utility of firm j evaluated at the Nash equilibrium security level solution, as discussed in Section 2.1. $E(U_j^{NE})$ is the disagreement point of firm j, according to the bargaining framework.

The objective function underlying the Nash bargaining model of cybersecurity investments is:

$$Z^1 = \prod_{j=1}^{m}(E(U_j(s)) - E(U_j^{NE})). \tag{20}$$

The optimization problem to be solved is then:

$$\text{Maximize} \prod_{j=1}^{m}(E(U_j(s)) - E(U_j^{NE})) \tag{21}$$

subject to:

$$-E(U_j(s)) \leq -E(U_j^{NE}), \quad j = 1, \ldots, m, \tag{22}$$

$$s \in K^1. \tag{23}$$

We define the feasible set K^2 consisting of constraints (22) and (23). Under our previous assumptions, we know that it is convex.

A solution to our Nash bargaining model is guaranteed to exist since the feasible set K^2 is compact and the objective function is continuous. We now provide conditions under which the solution is unique.

Theorem 3: Uniqueness of the Nash Bargaining Solution

The solution to the above cooperative Nash bargaining model is unique if the objective function, Z^1, is strictly quasi-concave.

Proof: This result follows from classical nonlinear programming theory. □

We now discuss a condition for which Z^1 will be strictly quasi-concave.

We can transform Z^1 as in (20) through the following logarithmic transformation:

$$ln(Z^1) = ln(\prod_{j=1}^{m}(E(U_j(s)) - E(U_j^{NE}))) = \sum_{j=1}^{m} ln(E(U_j(s)) - E(U_j^{NE})). \tag{24}$$

The objective function Z^1 is strictly quasi-concave if $ln(Z^1)$ is strictly concave.

2.3 The System-Optimization Model of Cybersecurity Investments

Under system-optimization, the objective function becomes:

$$Z^2 = \sum_{j=1}^{m} E(U_j(s)) \tag{25}$$

and the feasible set remains as for the Nash equilibrium problem, that is, $s \in K^1$.

Hence, the system-optimization cybersecurity investment problem is to:

$$\text{Maximize} \sum_{j=1}^{m} E(U_j(s)) \tag{26}$$

subject to:

$$s \in K^1. \tag{27}$$

We know that the feasible set K^1 is convex and compact and that the objective function (25) is continuous. Hence, the solution to the above system-optimization problem is guaranteed to exist. In addition, we have the following uniqueness result under an assumption.

Theorem 4: Uniqueness of the System-Optimized Solution

The solution to the system-optimization problem above is unique if the objective function, Z^2, is strictly quasi-concave.

Proof: The result follows from classical nonlinear programming theory. □

We now provide conditions under which the strict concavity of Z^2 will hold.

We construct:

$$\frac{\partial Z^2}{\partial s_j} = -\frac{\alpha_j}{2(1-s_j)^{1.5}} - [f_j(W_j) - f_j(W_j - D_j)][\frac{1}{m}\sum_{l=1}^{m} s_l + \frac{s_j - 1}{m} - 1]$$

$$- \sum_{k=1; j\neq k}^{m} \frac{s_k - 1}{m}[f_k(W_k) - f_k(W_k - D_k)]. \tag{28}$$

Also,

$$\frac{\partial^2 Z^2}{\partial s_j^2} = -\frac{3\alpha_j}{4(1-s_j)^{2.5}} - \frac{2}{m}[f_j(W_j) - f_j(W_j - D_j)], \tag{29}$$

and

$$\frac{\partial^2 Z^2}{\partial s_k \partial s_j} = \frac{\partial^2 Z^2}{\partial s_j \partial s_k} = -\frac{1}{m}[f_j(W_j) - f_j(W_j - D_j)] - \frac{1}{m}[f_k(W_k) - f_k(W_k - D_k)], \quad \text{for } k \neq j. \tag{30}$$

Z^2 is strictly concave if its Hessian matrix, H, is negative definite or $-H$ is positive definite (for all feasible s), where

$$H = \begin{bmatrix} \frac{\partial^2 Z^2}{\partial s_1^2} & \cdots & \frac{\partial^2 Z^2}{\partial s_1 \partial s_m} \\ \vdots & & \vdots \\ \frac{\partial^2 Z^2}{\partial s_m \partial s_1} & \cdots & \frac{\partial^2 Z^2}{\partial s_m^2} \end{bmatrix},$$

with the individual components for H as in (29) and (30) above. This matrix is symmetric. Moreover, we know that $-H$ is positive definite if it is strictly diagonally dominant, with the satisfaction of the condition below:

$$\frac{3\alpha_i}{4(1-s_i)^{2.5}} > \frac{m-3}{m}[f_i(W_i) - f_i(W_i - D_i)] + \frac{1}{m} \sum_{j=1; j \neq i}^{m} [f_j(W_j) - f_j(W_j - D_j)], \quad j = 1, \ldots, m. \tag{31}$$

One can deduce, for example, that (31) will always be satisfied for $m = 2$ when $[f_i(W_i) - f_i(W_i - D_i)] = [f_j(W_j) - f_j(W_j - D_j)], \forall j \neq i$. This is useful since, if this relationship is true, strict diagonal dominance will always exist for two firms. However, if this relationship is not true and (31) holds, the matrix will still be positive definite. For $m = 3$, condition (31) is also useful.

3. Numerical Examples

In this Section, we present numerical examples/cases illustrating the cybersecurity investment models developed in Section 2. Solutions of the Nash Equilibrium model were computed by applying the Euler method as outlined in subsection 2.1, with the Euler method implemented in Matlab on a Lenovo G410 laptop with an Intel Core i5 processor and 8GB RAM. The convergence tolerance was set to 10^{-5}, so that the algorithm was deemed to have converged when the absolute value of the difference between each successively computed security level was less than or equal to 10^{-5}. The sequence $\{a_\tau\}$ was set to: $.1\{1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, ...\}$. We initialized the Euler method by setting the security levels at their lower bounds. The upper bounds on the security levels $u_{s_i} = 0.99, \forall i$.

The solutions to the Nash Bargaining and System-Optimization models were computed by applying the Interior Point Method in the SAS NLP Solver. The algorithm was called upon while using SAS Studio, a web browser-based programming environment. The maximum optimality error, in each case example below, was 5×10^{-7} for the S-O solutions. The optimality error is defined as the maximum violation of the constraints in the models. The optimality errors in the solution of the NB model in the cases below are reported with the solutions. For both NB and S-O, the solver was initialized at the lower bounds of the security levels.

Below we present cases illustrating two different industries: retail and financial services respectively. The industry aspect affects the firm size, wealth, and the damage parameters. Wealth, damages, and investment costs are given in US dollars in millions. The α_i values in the cybersecurity investment functions across all examples are the number of employees in millions based on the most recently available public data.

Case I: Retailers

In Case I, we consider two retailers. Firm 1 represents the second largest discount retailer in the United States, Target Corporation. The firm, in January 2014, announced that the security of 70 million of its users was breached and their information compromised. Credit card information of 40 million users was used by hackers to generate an estimated \$53.7 million in the black market as per Tobias (2014). Firm 2 represents The Home Depot, a popular retailer in the home improvement and construction domain. Products available under these categories are also sold through Target which makes them compete for a common consumer base. The company was struggling with high turnover and old software which led to a compromise of 56 million users (Tobias (2014)). Firm 1 suffered \$148 million in damages, according to the Consumer Bankers Association and the Credit Union National Association (Tobias (2014)). Home Depot incurred \$62 million in legal fees and staff overtime to deal with their cyber attack in 2014. Additionally, it paid \$90 million to banks for re-issuing debit and credit cards to users who were compromised (Tobias (2014)).

We use the annual revenue data for the firms to estimate their wealth. Hence, in US\$ in millions, $W_1 = 72600$; $W_2 = 78800$. The potential damages these firms stand to sustain in the case of similar cyberattacks as above in the future amount to (in US\$ in millions): $D_1 = 148.0$; $D_2 = 152$.

As in Shetty et al. (2009), we assume that the wealth functions are of the following form:

$$f_1(W_1) = \sqrt{W_1}; \quad f_2(W_2) = \sqrt{W_2}.$$

The cybersecurity investment cost functions are:

$$h_1(s_1) = 0.25(\frac{1}{\sqrt{1-s_1}} - 1); \quad h_2(s_2) = 0.30(\frac{1}{\sqrt{1-s_2}} - 1).$$

The parameters $\alpha_1 = .25$ and $\alpha_2 = .30$ are the number of employees of the respective firms in millions, thereby, representing their size.

Results for the Nash Equilibrium model, the Nash Bargaining model, and the System-Optimization model for cybersecurity investments are summarized in Table 1. Recall that the values of the expected utilities are in million of dollars.

Solution	**NE**	**NB**	**S-O**
s_1	0.384	0.443	0.460
s_2	0.317	0.409	0.388
v_1	0.616	0.557	0.540
v_2	0.683	0.591	0.612
$\bar{s}$	0.350	0.426	0.424
$\bar{v}$	0.650	0.574	0.576
$E(U_1)$	269.265	269.271	269.268
$E(U_2)$	280.530	280.531	280.534

Table 1: Results for NE, NB, and S-O for Target and Home Depot

We now discuss uniqueness of the NE solution in Table 1. Referring to the strict diagonal dominance condition (16), we observe that the diagonal elements of the Jacobian J above (16) will assume their lowest values at $s_i = 0$; $i = 1, 2$, in this example. Hence, if the strict diagonal dominance condition holds at these values of the security levels, it will hold over all values in the feasible set. We now let $b_i = \frac{3\alpha_i}{4(1-s_i)^{2.5}}$, and $c_i = \frac{m-5}{2m}[f_i(W_i) - f_i(W_i - D_i)] + \frac{1}{2m}\sum_{j=1;j\neq i}^{m}[f_j(W_j) - f_j(W_j - D_j)]$ for $i = 1, 2$. Hence, b_1 at $s_1 = 0$, is equal to .188, and $c_1 = -.138$. Similarly, b_2 at $s_2 = 0$, is equal to .225 and $c_2 = -.134$. Clearly, $b_1 > c_1$ and $b_2 > c_2$ and, therefore, the above NE security level pattern is unique.

We also evaluated the Hessian of $ln(Z^1)$ (cf. (24)), which is a symmetric matrix, for the NB problem and computed the eigenvalues and the lowest eigenvalue of minus the Hessian evaluated at the computed NB solution was: 321.315 and, therefore, the NB solution is locally unique.

We now turn to examining whether the solution to the S-O problem in Table 1 is unique. In particular, we refer to (31). We retain the definition of b_i as above for $i = 1, 2$, and define now d_i: $g_i = \frac{m-3}{m}[f_i(W_i) - f_i(W_i - D_i)] + \frac{1}{m}\sum_{j=1;j\neq i}^{m}[f_j(W_j) - f_j(W_j - D_j)]$, $i = 1, 2$. We know, from the above computation, that $b_1 = .188$, and we determine $g_1 = -.002$. Also, we know that $b_2 = .225$, from the above, with $g_2 = .002$. Clearly, we have that $b_1 > g_1$ and $b_2 > g_2$ and, therefore, condition (31) is satisfied so the S-O solution for the security levels is unique for this example.

As reported in Table 1, Nash equilibrium security level for Firm 1 is 0.384 and that for Firm 2 is .317, indicating that neither firm may be well-prepared to ward off against cyber threats. The network security is .35 and the network vulnerability is .65. Firm 2 achieves a higher expected utility than Firm 1 under the Nash Equilibrium solution.

The solution to the Nash Bargaining model, in which the firms collaborate on security levels, shows an increase in the security levels for each firm. The security level of Firm 1 increases from 0.384 to 0.443 and that of Firm 2 increases from 0.317 to 0.409. These increases also result in slightly higher expected utilities for both firms as compared to the values at their NE solution; thus, creating a win-win situation for the retailers and their consumers (who benefit from higher security levels). The network vulnerability decreases from .650 to .574, a marked decline. The optimality error for the NB solution was 3.17×10^{-7}.

We observe an increase of 6000 in expected utility of Target and 1000 for Home Depot if the firms employ NB as compared to NE. Comparison of S-O and NB shows an increase of 3000 for Home Depot but a decrease of 3000 for Target. Results for the S-O model reveal that, while the security level of Firm 1 increases, that of Firm 2 decreases, as compared to the NB solution. The network vulnerability increases. Also, the expected utility for Firm 1 is lower under the S-O solution concept than under the NB one, whereas that for Firm 2 is slightly higher under the S-O solution concept.

Target Corporation is part of the Retail Cyber Intelligence Sharing Center through which the firm shares cyber threat information with other retailers that are part of the Retail Industry Leaders Association and also with public stakeholders such as the U.S. Department of Homeland Security, and the FBI (RILA (2014)). Even Home Depot has expressed openness towards the sharing threat information.

Note that the results for the Nash Bargaining model are close to those for the System-Optimization model. The S-O model, however, operates on the premise that the firms are controlled by a single entity, thereby, making it an unlikely scenario in practice.

In order to further examine the magnitude of the possible changes in network vulnerability and expected utilities, we now report the results for sensitivity analysis for varying damage parameters but with the wealth parameters the same as in Table 1, and $\alpha_1 = 100.00, \alpha_2 =$

120.00. This would represent a big increase in the number of employees of the two firms and more damaging attacks. The expected utilities for both firms are reported in Table 2 under the three solution concepts. In Table 3, we report the computed security levels and the network vulnerability values.

Condition (16) holds for all the NE solutions in the sensitivity analysis as does condition (31) for the S-O solutions, where, as for the baseline example, the evaluation is done at the security levels equal to zero, since this would be the most restrictive.

Parameters		**NE**		**NB**		**S-O**	
D_1	D_2	$E(U_1)$	$E(U_2)$	$E(U_1)$	$E(U_2)$	$E(U_1)$	$E(U_2)$
24800	25200	222.472	235.991	223.541	237.087	223.410	237.220
34800	35200	210.460	223.098	211.619	224.278	211.517	224.381
44800	45200	200.039	212.090	201.276	213.340	201.212	213.405

Table 2: Expected Utilities for NE, NB, and S-O for Target and Home Depot for Varying D_i Parameters with $\alpha_1 = 100$ and $\alpha_2 = 200$

Parameters		**NE**			**NB**			**S-O**		
D_1	D_2	s_1^*	s_2^*	$\bar{v}$	s_1^*	s_2^*	$\bar{v}$	s_1^*	s_2^*	$\bar{v}$
24800	25200	.169	.066	.88285	.262	.164	.78711	.265	.161	.78719
34800	35200	.289	.197	.75705	.369	.281	.67496	.371	.279	.67502
44800	45200	.374	.288	.66915	.444	.363	.59661	.445	.362	.59665

Table 3: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for Target and Home Depot for Varying D_i Parameters with $\alpha_1 = 100$ and $\alpha_2 = 200$

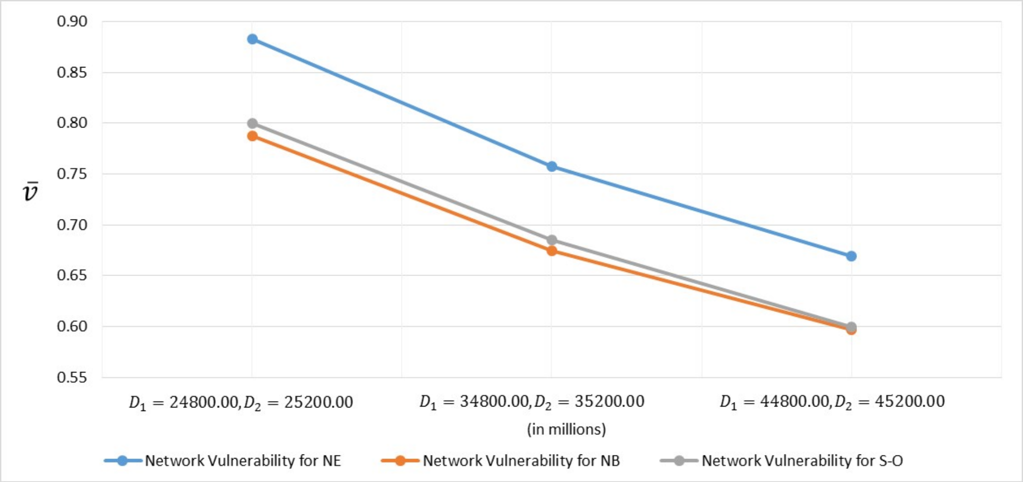

Figure 1: Representation of Table 3 Showing Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O with Varying D_i Parameters with $\alpha_1 = 100$ and $\alpha_2 = 200$

For both Target and Home Depot, an increase of over a million is observed on employing NB as compared to NE when $D_1 = 44800, D_2 = 45200$. Also, as illustrated in Table 5 and Figure 1, the network vulnerability is at 0.60 for NB and 0.67 for NE when $D_1 = 44800, D_2 = 45200$, which indicates that there is a significant decline in the vulnerability of the overall network if firms cooperate. The optimality error for the NB solutions was 5×10^{-7}.

Minus the Hessian of $ln(Z^1)$, a symmetric matrix, evaluated at the NB solutions of all the sensitivity analysis examples discussed above had positive eigenvalues, implying that they were positive definite. Hence, the NB solutions in Tables 2 and 3 are locally unique.

As the number of employees have increased, the investment cost functions for both firms increased and, hence, the security levels dropped as compared to Table 1. However, the varying increase in damages, as shown in Tables 2 and 3, is leading to an increase in the security levels. The network vulnerability is consistently the lowest for the NB solution concept, demonstrating the benefit of bargaining for cooperation in cybersecurity.

For Home Depot, an increase of 1.25 million in expected utility is observed on employing NB as compared to NE and for Target, an increase of 1.24 million is observed when $D_1 = 44800, D_2 = 45200$, which is the highest of the three scenarios evaluated through our sensitivity analysis. Clearly, the reported increase is much higher than in Table 1 and Table 2. Comparison of S-O and NB shows an increase of 64,432 for Target but a decrease of 64,081 for Home Depot when $D_1 = 44800, D_2 = 45200$.

Case II: Financial Service Firms

In Case II we consider three banking and financial service firms. Firm 1 represents the largest bank in the United States, JPMorgan Chase (JPMC). Cyber intrusion faced by the bank was one of the largest ever and one of the most talked about in 2014. More than 76 million households and seven million small businesses were compromised. The bank's forensics investigations revealed that hackers had obtained a list of applications and programs run by JPMC and found alternate entry points to penetrate the systems (Silver-Greenberg, Goldstein, and Perlroth (2014)).

Firm 2 represents the third largest bank in the United States, Citibank, part of Citigroup. The bank has reported violation through cyber means in multiple instances in the past few years. However, to focus on one such event, we discuss the reported breach in 2011 in which 34,000 of the company's customers were affected. Financial losses were compensated by the company and 217,657 credit cards were replaced to ensure safety (Neowin (2011)).

Firm 3 is represented by HSBC Holdings Plc's Turkish Unit. Inclusion of the company gives an international angle to the analysis, especially since vulnerability of Turkey's HSBC can be manipulated to penetrate HSBC in the UK, United States, Canada, and so on. The unit was attacked right after JPMC in 2014 and 2.7 million customers' bank data was lost (Bloomberg (2014)).

In US$ in millions, $W_1 = 51500$; $W_2 = 33300$; $W_3 = 31100$. Since HSBC Holdings Plc in its entirety would battle against an attack on any of its units, the wealth of HSBC Holdings is considered instead of just the Turkish unit. The potential damages these firms could stand to sustain in the future, in the case of similar cyberattacks to those described above, amount to (in US$ in millions): $D_1 = 250.00$; $D_2 = 172.80$; $D_3 = 580.50$. Damage for Firm 1 is estimated based on its spending after cybersecurity in 2014 since the firm claims to not have registered complaints of actual damage from customers. For Firm 2, it was assessed that loss per customer was \$794 US (Neowin (2011)). A survey from the Ponemon Institute (2013) states that per record cost for a cyberattack on financial firms was \$215 US in 2012. Damage for Firm 3 is estimated based on this data and the fact that 2.7 million customers were compromised.

The wealth functions are:

$$f_1(W_1) = \sqrt{W_1}; \quad f_2(W_2) = \sqrt{W_2}; \quad f_2(W_3) = \sqrt{W_3}.$$

The cybersecurity investment cost functions take the form:

$$h_1(s_1) = 0.27(\frac{1}{\sqrt{1-s_1}} - 1); \quad h_2(s_2) = 0.24(\frac{1}{\sqrt{1-s_2}} - 1); \quad h_3(s_3) = 0.27(\frac{1}{\sqrt{1-s_3}} - 1).$$

The α_i; $i = 1, 2, 3$ values in the investment cost functions (cf. (2)) represent the total number of employees of the organizations in millions. As of 2014, the number of employees in JPMC was approximately 265000, the number in Citigroup was 243000, and that in HSBC Holdings Plc: 263273. Hence, we have set $\alpha_1 = .27$, $\alpha_2 = .24$, and $\alpha_3 = .27$. Since these illustrate the size of the organizations and the number of employees that will need to be protected (and trained) in order to ward off cyber attacks on the organizations and, thus, consumers, they are included in the investment cost functions.

The results for the Nash Equilibrium model, the Nash Bargaining model, and the System-Optimization model for cybersecurity investments are summarized in Table 4.

We first verify whether or not the Nash Equilibrium solution s^* in Table 4 is unique. We use the definitions of the b_i and c_i as given in Case I (and evaluated at security levels equal

Solution	**NE**	**NB**	**S-O**
s_1	0.467	0.542	0.581
s_2	0.454	0.535	0.598
s_3	0.719	0.762	0.718
v_1	0.533	0.458	0.419
v_2	0.547	0.465	0.402
v_3	0.281	0.238	0.282
$\bar{s}$	0.546	0.613	0.632
$\bar{v}$	0.454	0.387	0.368
$E(U_1)$	226.703	226.709	226.704
$E(U_2)$	182.281	182.286	182.274
$E(U_3)$	175.902	175.916	175.942

Table 4: Results of NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit

to zero) and compute them for this example with three firms for $i = 1, 2, 3$. Specifically, we have that: $b_1 = .202$, $c_1 = .171$, $b_2 = .180$, $c_2 = .209$, and $b_3 = .520$, with $c_3 = -.380$. Clearly, for this example, we have that: $b_1 > c_1$ and $b_3 > c_3$. However, $b_2 < c_2$ so we cannot guarantee that condition (16) is satisfied, unlike for the baseline example for Case I. Recall that the strict diagonal dominance condition guarantees that a matrix is positive definite but a matrix may be positive definite even if the strict monotonicity condition does not hold. Indeed, if all the eigenvalues of a symmetric matrix are positive, then positive definiteness of the matrix is guaranteed. We evaluate the eigenvalues for $\frac{1}{2}(J + J^T)$ and find that the smallest eigenvalue is positive and equal to .699. Hence, uniqueness of the NE cybersecurity level investment solution in Table 4 is guaranteed.

We also know that the NB solution in Table 4 is locally unique since we evaluated the Hessian of (24) and the smallest eigenvalue of minus that Hessian is: 501.665.

When we evaluate condition (31), which corresponds to the strict diagonal dominance condition holding for the corresponding Hessian matrix $-H$ we find that for this example, the condition does not hold. Nevertheless, the smallest eigenvalue of this matrix is positive and equal to .044. Consequently, we know that the S-O solution reported in Table 4 is unique.

In terms of the NE solution, Firm 3 has the highest security level and Firm 2 the lowest. Firm 1 enjoys the highest expected utility and Firm 3 the lowest. Similar to the results for Case I, we observe lower security levels for the firms with more wealth. For JPMC, we observe an increase of 6000 in expected utility, 1000 for Citibank and 14,000 for HSBC when NB is employed as opposed to NE. Comparison of S-O and NB shows an increase of 26,000 for HSBC but a decrease of 5000 for JPMC and 12,000 for Citibank. The expected utility of Citibank through the S-O solution concept is 7000 below that under the NE concept.

In the results for the NB model, we observe that the security levels of all three firms are higher than their respective security levels for the Nash Equilibrium model. Consequently, the network vulnerability is decreased to 0.387 from 0.454. The optimality error for the NB solution is 9.86×10^{-6}.

Quantum Dawn 2 and 3 are cybersecurity incident response drills conducted for enhancing resolution and coordination processes in the financial services sector. These exercises are meant to avoid ripple effects of a cyberattack on one firm to others. To counteract such coordinated attacks, the financial service firms and banks realize the importance of sharing information and protect through a coordinated response (SIFMA (2015)). Our results on Nash bargaining corroborate this understanding, support negotiations, and numerically reveal the increase in security levels and the concomitant decrease in network vulnerability.

As noted earlier, since the goal of the System-Optimization model is to maximize the sum of the expected utilities and not necessarily to enhance the security level of the network, the individual security levels adjust so that the total expected utility is higher than those obtained through the other models. However, individually, Firm 1 and Firm 2 have lower expected utilities than they had through thee Nash Bargaining solution concept. Also, Firm 2 has an expected utility lower than that under the Nash Equilibrium.

In order to further examine the magnitude of changes in network vulnerability and expected utilities, we now report results of sensitivity analysis if the wealth parameters are the same as in Table 4, but with damage parameters increased to $D_1 = 25000.00, D_2 = 17200.80, D_3 = 28000.50$, and the alpha parameters varying in an elevated range. Such increases represent more damaging attacks on the firms. The expected utilities are reported in Table 5 and the computed security levels and network vulnerability values are reported in Table 6.

Parameters			**NE**			**NB**			**S-O**		
α_1	α_2	α_3	$E(U_1)$	$E(U_2)$	$E(U_3)$	$E(U_1)$	$E(U_2)$	$E(U_3)$	$E(U_1)$	$E(U_2)$	$E(U_3)$
75	65	75	183.136	144.520	105.422	184.644	145.827	107.881	184.040	144.016	111.114
100	90	100	177.133	139.292	92.330	179.045	140.963	95.448	178.276	138.697	99.500
150	125	150	170.457	133.215	72.735	173.065	135.456	76.988	172.027	132.289	82.638

Table 5: Expected Utilities for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit for Varying α_i Parameters with $D_1 = 25000.00, D_2 = 17200.80$ and $D_3 = 28000.50$

Parameters			**NE**				**NB**				**S-O**			
α_1	α_2	α_3	s_1^*	s_2^*	s_3^*	$\bar{v}$	s_1^*	s_2^*	s_3^*	$\bar{v}$	s_1^*	s_2^*	s_3^*	$\bar{v}$
75	65	75	.258	.258	.484	.66673	.366	.366	.564	.56793	.392	.423	.513	.55717
100	90	100	.169	.151	.423	.75226	.291	.275	.512	.64082	.319	.339	.456	.62874
150	125	150	.018	.040	.318	.87477	.161	.180	.423	.74504	.195	.257	.356	.73086

Table 6: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit for Varying α_i Parameters with $D_1 = 25000.00, D_2 = 17200.80$ and $D_3 = 28000.50$

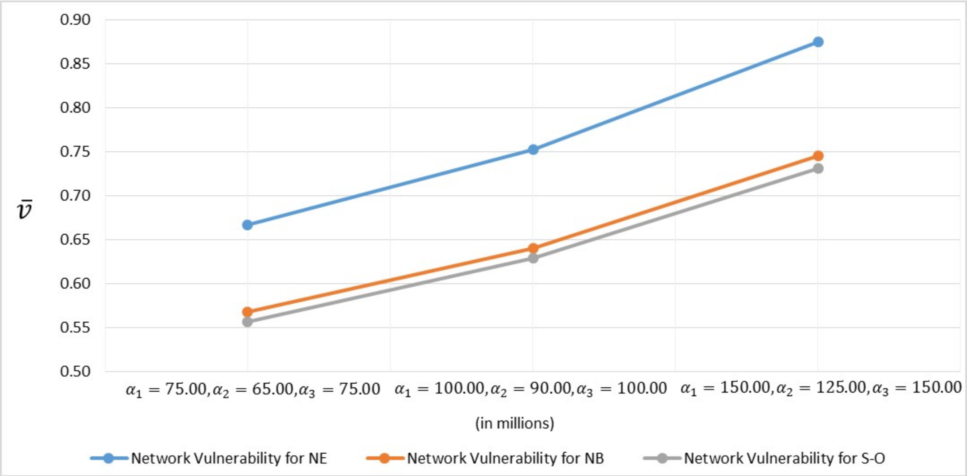

Figure 2: Representation of Table 6 Showing Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O with Varying α_i Parameters with $D_1 = 25000.00, D_2 = 17200.80$ and $D_3 = 28000.50$

As illustrated in Figure 2, the network vulnerability is the lowest in the case of the S-O solutions. However, for Citibank, we observe that the expected utilities for every set of alpha parameters are lower than their corresponding NE values. These results are similar to those in Table 4. For the third scenario, the expected utility of Citibank is 133.215 million for NE, 135.456 million for NB, and 132.289 million for S-O. A firm such as Citibank would not prefer an S-O approach if it possibly could attain a utility 927,000 below the value when it competes. But as per constraint (23), NB leads to better expected utilities for all three firms and a network vulnerability significantly lower than NE. The optimality error for the NB solutions was 9.40×10^{-7}.

Conditions (16) and (31) were evaluated for all the sensitivity analysis examples above at the solutions and for security levels equal to zero, which is the most restrictive. The conditions are met, and, thus, the solutions are unique.

Minus the Hessian of $ln(Z^1)$, a symmetric matrix, evaluated at the NB solutions of all the sensitivity analysis examples discussed above had positive eigenvalues, implying that they were positive definite. Hence, the NB solutions in Tables 5 and 6 are locally unique.

For JPMC, an increase of 2.61 million in expected utility is observed on employing NB as compared to NE; for Citibank, an increase of 2.24 million and for HSBC, an increase of 4.25 million is observed when $\alpha_1 = 150, \alpha_2 = 125, \alpha_3 = 150$, which constitute the highest of the three scenarios evaluated above. Comparison of S-O and NB shows an increase of 5.65 million for HSBC but a decrease of 1.04 million for JPMC and 3.17 million for Citibank when $\alpha_1 = 150, \alpha_2 = 125, \alpha_3 = 150$.

Since the wealth and damage parameters influence the network vulnerability and expected utilities, we take into consideration another situation wherein the parameters are the same for all three firms. They are fixed as follows: $W_1 = 51500, W_2 = 51500, W_3 = 51500; D_1 = 25000, D_2 = 25000, D_3 = 25000$. The expected utilities are reported in Table 7 and the computed security levels and network vulnerability values are reported in Table 8.

Parameters			**NE**			**NB**			**S-O**		
α_1	α_2	α_3	$E(U_1)$	$E(U_2)$	$E(U_3)$	$E(U_1)$	$E(U_2)$	$E(U_3)$	$E(U_1)$	$E(U_2)$	$E(U_3)$
50	50	50	189.012	189.012	189.012	190.253	190.253	190.253	190.253	190.253	190.253
50	75	50	187.406	184.183	187.406	188.741	185.647	188.741	188.529	186.091	188.529
50	100	25	188.116	184.881	196.217	189.316	186.288	197.243	189.032	187.397	196.560

Table 7: Expected Utilities for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit for Varying α_i Parameters with $D_1 = 25000, D_2 = 25000$ and $D_3 = 25000$

Parameters			**NE**				**NB**				**S-O**			
α_1	α_2	α_3	s_1^*	s_2^*	s_3^*	$\bar{v}$	s_1^*	s_2^*	s_3^*	$\bar{v}$	s_1^*	s_2^*	s_3^*	$\bar{v}$
50	50	50	.389	.389	.389	.61140	.480	.480	.480	.51987	.480	.480	.480	.51987
50	75	50	.404	.249	.404	.64780	.494	.358	.494	.55129	.500	.345	.500	.55150
50	100	25	.397	.110	.598	.63157	.488	.230	.661	.54062	.494	.198	.682	.54215

Table 8: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit for Varying α_i Parameters with $D_1 = 25000, D_2 = 25000$ and $D_3 = 25000$

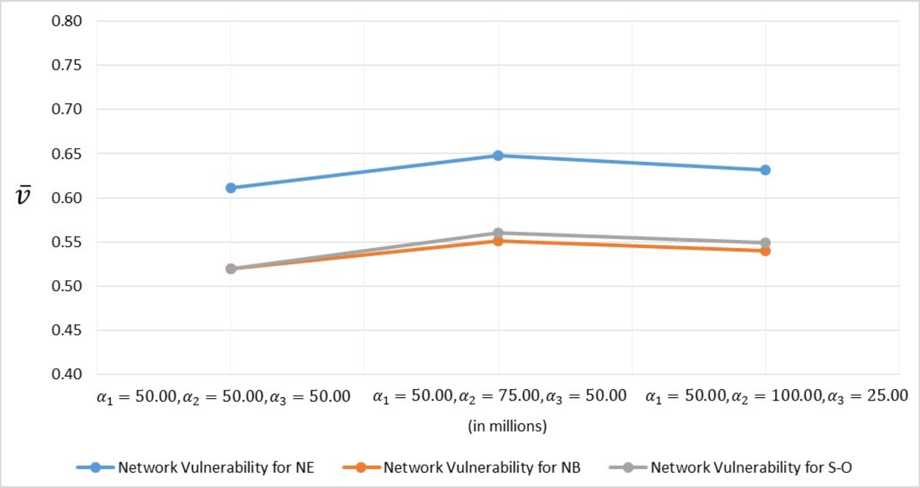

Figure 3: Representation of Table 8 Showing Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O and Varying α_i Parameters with $D_1 = 25000, D_2 = 25000$ and $D_3 = 25000$

In the first scenario, in which $\alpha_1 = \alpha_2 = \alpha_3$, the expected utilities and network vulnerability for the NB and the S-O solutions are the same. Hence, if all the firms have equal wealth, damages, and size, either the NB or the S-O approach can be adopted. Yet, the potential to obtain a lower network vulnerability through NB gets highlighted as the size of the firms (or the $\alpha_i; i = 1, 2, 3$) changes. The optimality error for the NB solutions was 3.53×10^{-7}. Through bargaining, the firm of larger size attains a higher security level as compared to during system-optimization.

Based on Cases I and II, which describe results for different industrial sectors along with their sensitivity analysis, it can be stated that the Nash Bargaining model is the most practical and beneficial for firms, the network, and consumers alike in terms of security levels. Moreover, the expected utilities of the firms under NB are always greater than or equal to the respective ones under the NE solution, demonstrating that the firms' individual expected profits do not suffer under cooperation as per Nash Bargaining.

4. Summary and Conclusions

In this paper, we explored cybersecurity investments in the case of multiple firms in the same industrial sector and presented three new models. In the first model, the governing concept was that of Nash Equilibrium with the firms competing in terms of their cybersecurity levels. In the second model, the governing concept was that of Nash Bargaining, in which the disagreement point was the Nash equilibrium. In this model, the constraints included not only the bounds on the security levels but also that the expected utility for each firm could not be lower than that achieved under the Nash equilibrium solution. The objective function for this model was the product over all the firms of each firm's expected utility minus its expected utility evaluated at the Nash equilibrium. The third model was also one of cooperation, and the concept was that of System-Optimization in which the sum of the expected utilities of all firms was maximized.

The Nash equilibrium was formulated as a variational inequality problem and an algorithm proposed for its solution since an associated optimization reformulation does not exist. Qualitative properties of existence and uniqueness were examined and obtained for all models.

We then investigated the models through two case studies focusing on different industrial sectors in which cyberattacks have been prominent recently; in particular, the retail sector and the financial services sector. We computed solutions to all three cybersecurity investment models for each case and determined the security levels of the firms, their individual vulnerability as well as the vulnerability of their networks, and their expected utilities. Since the wealth, damage, and alpha parameters significantly affect the security levels, network vulnerability, and expected utilities, we conducted sensitivity analysis for all three cases.

In Case I, we first computed the results based on estimated data for two major retailers, Target and Home Depot. The network vulnerability for NB was found to be the lowest out of the three solution concepts. To explore competition vs. cooperation, we conducted sensitivity analysis over the damage parameters with increasing alpha values associated with the cybersecurity investment cost functions. An increase as high as 1.24 million in expected utility was observed for Target and 1.25 million for Home Depot if NB was employed instead of NE.

For Case II, we computed the results based on estimated data for three financial service firms: JPMC, Citibank, and HSBC. The network vulnerability was the lowest in the case of S-O. However, expected utility of one of the firms fell below its corresponding NE value which made system-optimization a less appropriate solution concept even with lower network vulnerability. The magnitude of changes in expected utilities was reported through sensitivity analysis on the alpha parameters. Increases as high as 2.61 million for JPMC, 2.24 million for Citibank, and 4.25 million for HSBC in expected utility were observed if NB was adopted in place of NE. We also reported analysis over alpha parameters for the three firms for equal wealth and damage parameters. The results showed that if the wealth, damage, and alpha parameters of all firms were the same, either NB or the S-O approach could be taken. The benefits of bargaining, resulting in lower network vulnerability, also was highlighted as the sizes of the firms change.

Our results show that the Nash Bargaining concept yields enhanced network security in all industrial sector cases as compared to the Nash Equilibrium solution. Since firms bargain, the constraints guarantee that a not lower expected utility for each firm is ensured. This concept, with increasing emphasis on the sharing of cyber information, is the most pragmatic one since we can expect firms to negotiate among one another rather than be controlled by a central controller via system-optimization, where a firm may win and another lose as compared to the Nash Bargaining solution. Moreover, there is increasing pressure from the government and policy-makers to have firms exchange information in the cyber space as a possible defensive mechanism. Our results support cooperation among firms, which may otherwise be competitors, in terms of cybersecurity investments.

Acknowledgments

This research was supported, in part, by the National Science Foundation (NSF) grant CISE #1111276, for the NeTS: Large: Collaborative Research: Network Innovation Through Choice project and by the NSF EAGER grant #1551444: Collaborative Research: Enabling Economic Policies in Software-Defined Internet Exchange Points, awarded to the University of Massachusetts Amherst as well as by the John F. Smith Memorial Fund at the University of Massachusetts Amherst. This support is gratefully acknowledged.

The authors thank the two anonymous reviewers for their helpful comments and suggestions on two earlier versions of this paper.

References

Aggarwal P., Maqbool Z., Grover A., Pammi V.S., Singh S., & Dutt V. (2015). Cyber Security: A game-theoretic analysis of defender and attacker strategies in defacing-website games. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment, IEEE*, 1-8.

AON Risk Services and Ponemon Institute. 2015 global cyber impact report. (2015). http://www.aon.com/attachments/risk-services/2015-Global-Cyber-Impact-Report-Final .pdf/ Accessed 12.04.16.

Bakshi N, & Kleindorfer P. (2007). Co-opetition and investment for supply-chain resilience. *Production and Operations Management*, 18(6), 583-603.

Binmore K., Rubinstein A., & Wolinsky A. (1989). The Nash bargaining solution in economic modelling. *The Rand Journal of Economics* 17(2): 176-188.

Bloomberg. HSBC loses 2.7 million customers data in Turkey-attack. (2014). http://www.bloomberg.com/news/articles/2014-11-13/hsbc-loses-2-7-million-customers-data-in-turkey-attack/ Accessed 14.09.15.

Bloomberg. UglyGorilla hack of U.S. utility exposes cyberwar threat. (2014). http://www.bloomberg.com/news/articles/2014-06-13/uglygorilla-hack-of-u-s-utility-exposes-cyberwar-threat/ Accessed 02.09.15.

Boonen, T. J. (2016). Nash equilibria of over-the-counter bargaining for insurance risk redistributions: The role of a regulator. *European Journal of Operational Research*, 250(3), 955-965.

Center for Strategic and International Studies. Net losses: Estimating the global cost of cybercrime. (2014). http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf/ Accessed 12.04.16.

ComputerWeekly.com. Business disruption cyber attacks set to spur defence plans, says Gartner. (2015). http://www.computerweekly.com/news/2240241129/Business-disruption-cyber-attacks-set-to-spur-defence-plans-says-Gartner/ Accessed 12.04.16.

Daras N. J., & Rassias M. T. (2015). *Computation, Cryptography, and Network Security.* Switzerland: Springer International Publishing.

Das S. (2015). The Cyber Security Ecosystem: Post-global Financial Crisis. In *Managing in Recovering Markets* (pp. 453-459). New Delhi: Springer India.

Deloitte Center for Financial Services. Transforming cybersecurity: New approaches for an evolving threat landscape.(2014). http://www2.deloitte.com/content/dam/Deloitte/global /Documents/Financial-Services/dttl-fsi-TransformingCybersecurity-2014-02.pdf/ Accessed 12.04.16.

Dodd, V. Cyber-attack warning after millions stolen from UK bank accounts. (2015). http://www.theguardian.com/technology/2015/oct/13/nca-in-safety-warning-after-millions-stolen-from-uk-bank-accounts/ Accessed 10.09.15.

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

Gabay D., & Moulin H. (1980). On the uniqueness and stability of Nash equilibria in noncooperatiive games. In Bensoussan A., Kleindorfer P., & Tapiero C.S. (Eds.), *Applied Stochastic Control in Econometrics and Management Science* (pp. 271-294). North Holland:

Elsevier Science Ltd.

Garvey P.R., Moynihan R.A., & Servi L. (2013). A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach. *Systems Engineering* 16(3): 313-328.

Gordon L.A., Loeb M.P., Lucyshyn W., & Zhuo L. (2015). Externalities and the magnitude of cybersecurity underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security* 6: 24-30.

Granville, K. 9 recent cyberattacks against big businesses. (2015). http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html/ Accessed 12.09.15.

Harrington J.E., Hobbs B.F., Pang J.S., Liu A., & Roch G. (2005). Collusive game solutions via optimization. *Mathematical Programming* 104(2-3): 407-435.

Harsanyi J.C. (1977). *Rational Behavior and Bargaining Equilibrium in Games an Social Situations*. Cambridge: Cambridge University Press.

Jiang W., Zhang-Shen R., Rexford J., & Chiang M. (2009). Cooperative content distribution and traffic engineering in an ISP network. *ACM SIGMETRICS Performance Evaluation Review* 37(1): 239-250.

Kinderlehrer D., & Stampacchia G. (1980). *Variational Inequalities and their Applications*. New York: Academic Press.

Korpelevich G.M. (1977) The extragradient method for finding saddle points and other problems. *Matekon* 13: 35-49.

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

Leshem A., & Zehavi E. (2008). Cooperative game theory and the Gaussian interference channel. *IEEE Journal on Selected Areas in Communications* 26(7): 1078-1088.

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

McKinsey & Company Quarterly. The rising strategic risks of cyberattacks. (2014). http://www.mckinsey.com/business-functions/business-technology/our-insights/the-rising-strategic-risks-of-cyberattacks/ Accessed 12.04.16.

Muthoo A. (1999). *Bargaining Theory with Applications.* Cambridge: Cambridge University Press.

Nagarajan M., & Sosic G. (2008). Game-theoretic analysis of cooperation among supply chain agents: Review and extensions. *European Journal of Operational Research* 187(3): 719-745.

Nagurney A. (1999). *Network Economics: A Variational Inequality Approach.* (2nd and revised ed.). Boston: Kluwer Academic Publishers.

Nagurney A. (2006). *Supply Chain Network Economics: Dynamics of Prices, Flows and Profits.* Cheltenham: Edward Elgar Publishing.

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

Nagurney A., Daniele P., & Shukla S. (2016). A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of Operations Research.* doi:10.1007/s10479-016-2209-1.

Nagurney A., & Nagurney L.S. (2015). A game theory model of cybersecurity investments with information asymmetry. *Netnomics* 16(1-2): 127-148.

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

Nagurney A., & Zhang D. (1996). *Projected Dynamical Systems and Variational Inequalities with Applications.* Boston: Kluwer Academic Publishers.

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

Nash J.F. (1950b). The bargaining problem. *Econometrica* 18: 155-162.

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

Nash J.F. (1953). Two person cooperative games. *Econometrica* 21: 128-140.

Neowin. $2.7 million stolen in Citigroup hack attack. (2011). http://www.neowin.net/news/27-million-stolen-in-citigroup-hack-attack/ Accessed 11.09.15.

Patrascu A., & Simion E. (2014). Applied cybersecurity using game theory elements. *Proceedings of 10th International Conference on Communications, IEEE*, 1-4.

Ponemon Institute. 2013 cost of data breach study: Global analysis. (2013). https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf/ Accessed 12.04.16.

Ponemon Institute. 2015 cost of cybercrime study: United States. (2015). http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states/ Accessed 12.04.16.

RAND Security Division. Markets for cybercrime tools and stolen data. (2014). http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf/ Accessed 12.04.16.

RILA. Retailers launch comprehensive cyber intelligence sharing center. (2014). http://www.rila.org/news/topnews/Pages/RetailersLaunchComprehensiveCyber Intelligence-SharingCenter.aspx/ Accessed 12.09.15.

SIFMA. SIFMA statement on completion of the Quantum Dawn 3 cybersecurity exercise. (2015).
http://www.sifma.org/newsroom/2015/sifma-statement-on-completion-of-the-quantum-dawn-3-cybersecurity-exercise/ Accessed 10.09.15.

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

Shetty N., Schwartz G., Felegyhazi M., & Walrand J. (2010). Competitive cyber-insurance and internet security. In *Economics of Information Security and Privacy* (pp. 229-247). New York: Springer US.

Silver-Greenberg, J., Goldstein, M, & Perlroth, N. JPMorgan Chase hacking affects 76 million households. (2014). http://dealbook.nytimes.com/2014/10/02/jpmorgandiscovers-further-cyber-security-issues/?-r=1/ Accessed 21.08.15.

Tatsumi, K. I., & Goto, M. (2010). Optimal timing of information security investment: A real options approach. In *Economics of Information Security and Privacy* (pp. 211-228). New York: Springer US.

Tobias, S. 2014: The year in cyberattacks. (2014). http://www.newsweek.com/2014-year-cyber-attacks-295876/ Accessed 14.09.15.

The Wall Street Journal. Retailers' dilemma: Innovation vs. cyber security risk. (2014). http://deloitte.-wsj.com/cio/2014/11/24/retails-digital-dilemma-innovation-vs-cyber-security-risk/ Accessed 12.09.15.

US Department of Energy. Energy department invests over $34 Million to improve protection of the nations energy infrastructure. (2015). http://www.energy.gov/-articles/energy-department-invests-over-34-million-improve-protection-nation-s-energy - infrastructure/ Accessed 14.09.15.

US Department of Homeland Security. Incident response/vulnerability coordination in 2014. (2015). National Cybersecurity and Communications Integration Center. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf/ Accessed 12.04.16.

USA Today. Regulator warns of 'Armageddon' cyber attack on banks. (2015). http://www.usatoday.com/story/money/business/2015/02/25/lawsky-goldman-sachs-banks /23995979/ Accessed 12.09.15.

Wagner S., Berg E.V.D., Giacopelli J., Ghetie A., Burns J., Tauil M., Lan T., Sen S., Wang M., Chiang M., Laddaga R., Robertson P., & Manghwani P. (2012). Autonomous, collaborative control for resilient cyber defense (ACCORD). *Sixth International Conference on Self-Adaptive and Self-Organizing Systems Workshops, IEEE*, 39-46.