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

Professor Anna Nagurney
Department of Operations and Information Management
Isenberg School of Management
University of Massachusetts Amherst
Professor Ladimer S. Nagurney
Department of Electrical and Computer Engineering
University of Hartford
Shivani Shukla
Department of Operations and Information Management
Isenberg School of Management
University of Massachusetts Amherst

INFORMS Annual Meeting, Nov 1-4, 2015, Philadelphia, PA

Outline

Introduction

- **Complex and globalized supply chains** have led to vulnerable IT infrastructure that affects firms and consumers.
- Estimated annual cost to the global economy from cybercrime is more than $400 billion, conservatively, $375 billion in losses, more than the national income of most countries (Center for Strategic and International Studies (2014)).

Introduction

- Growing interest in the development of **rigorous scientific tools**.
- Investments by one decision-maker may affect the decisions of others and the overall supply chain network security (or vulnerability) - Application of **Game Theory**.
- Holistic approach needed - **cyber supply chain risk management** (Boyson (2014)).

Approach

- A supply chain game theory model developed consisting of **two tiers: the retailers and the consumers**.

Approach

- A supply chain game theory model developed consisting of **two tiers: the retailers and the consumers**.

Approach

- A supply chain game theory model developed consisting of **two tiers: the retailers and the consumers**.
- Retailers seek to maximize their expected profits. **Price is a function of demand and average network security** in the supply chain.

Approach

- A supply chain game theory model developed consisting of **two tiers: the retailers and the consumers**.
- Retailers seek to maximize their expected profits. **Price is a function of demand and average network security** in the supply chain.
- The **probability of a successful attack** on a retailer depends not only on its own security level but also on security levels of other retailers.

Approach

- A supply chain game theory model developed consisting of **two tiers: the retailers and the consumers**.
- Retailers seek to maximize their expected profits. **Price is a function of demand and average network security** in the supply chain.
- The **probability of a successful attack** on a retailer depends not only on its own security level but also on security levels of other retailers.
- The **retailers compete noncooperatively until a Nash equilibrium** is achieved, whereby no retailer can improve upon his expected profit by making a unilateral decision in changing his product transactions and security level.

Approach

- A supply chain game theory model developed consisting of **two tiers: the retailers and the consumers**.
- Retailers seek to maximize their expected profits. **Price is a function of demand and average network security** in the supply chain.
- The **probability of a successful attack** on a retailer depends not only on its own security level but also on security levels of other retailers.
- The **retailers compete noncooperatively until a Nash equilibrium** is achieved, whereby no retailer can improve upon his expected profit by making a unilateral decision in changing his product transactions and security level.
- Retailers: are non-identical, can have distinct investment cost functions, can be spatially separated, brick and mortar/online.

Papers

The presentation is based on:

Nagurney, A., Nagurney, L.S., Shukla, S. (2015). A supply chain game theory framework for cybersecurity investments under network vulnerability. In *Computation, Cryptography, and Network Security*, Daras, Nicholas J., Rassias, Michael Th. (Eds.), Springer, 381-398.

Important References:

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

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

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

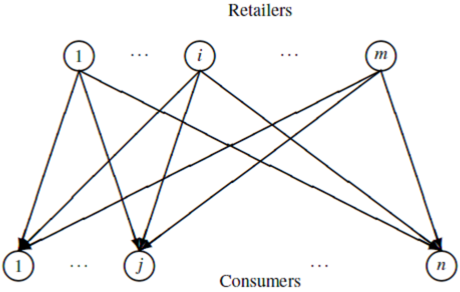

Fig. 1 The network structure of the supply chain game theory model

- m spatially separated retailers. Financial transaction through debit/credit cards.

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

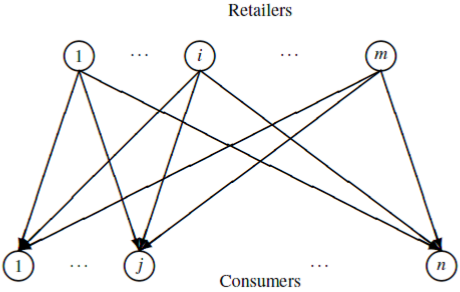

Fig. 1 The network structure of the supply chain game theory model

- m spatially separated retailers. Financial transaction through debit/credit cards.

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

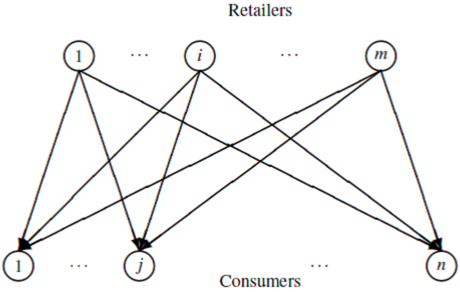

Fig. 1 The network structure of the supply chain game theory model

- m spatially separated retailers. Financial transaction through debit/credit cards.
- Cyberattack could cause financial damage, loss of reputation, identity theft, loss of opportunity cost, etc.

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

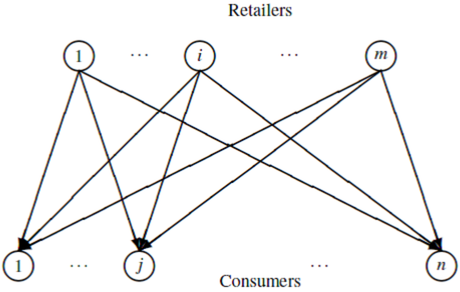

Fig. 1 The network structure of the supply chain game theory model

- m spatially separated retailers. Financial transaction through debit/credit cards.
- Cyberattack could cause financial damage, loss of reputation, identity theft, loss of opportunity cost, etc.
- 'Retailers' - Pharmaceutical, High Tech, Financial, etc.

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

Network Security, s_i:

$$0 \leq s_i \leq 1; \quad i = 1, ..., m.$$

Average Network Security of the Chain, $\bar{s}$:

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

Probability of a Successful Cyberattack on i, p_i:

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

Vulnerability, v_i:

$v_i = (1 - s_i), \quad i = 1, ..., m$. Vulnerability of network, $\bar{v} = (1 - \bar{s})$.

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

Investment Cost Function to Acquire Security s_i, $h_i(s_i)$:

$$h_i(s_i) = \alpha_i\left(\frac{1}{\sqrt{(1-s_i)}} - 1\right), \quad \alpha_i > 0, \qquad i = 1, \ldots, m.$$

α_i quantifies size and needs of retailer i; $h_i(0) = 0 =$ insecure retailer, and $h_i(1) = \infty =$ complete security at infinite cost. **Conservation of Flow:**

$$d_j = \sum_{j=1}^{n} Q_{ij}, \qquad j = 1, \ldots, n,$$

where

$$Q_{ij} \geq 0, \qquad \forall i, j.$$

Demand grouped into: $d \in R^n_+$.

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

Demand Price Function for Consumer j, ρ_j:

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

Demand price depends on quantity transacted and *average* network security. Consumers may not know about individual retailer's investments in cybersecurity. **Revenue of Retailer, i; $i = 1, ..., m$, in Absence of Cyberattack:**

$$\sum_{j=1}^{n} \hat{\rho}_j(Q, s) Q_{ij}, \quad \hat{\rho}_j(Q, s) \equiv \rho_j(d, \bar{s}).$$

Cost of Handling and Processing + Transaction:

$$c_i \sum_{j=1}^{n} Q_{ij} + \sum_{j=1}^{n} c_{ij}(Q_{ij}), \quad i = 1, ..., m.$$

Above is assumed to be convex and continuously differentiable.

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

Profit of Retailer in absence of cyberattack and investments, f_i:

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

Incurred financial damage: D_i.

Expected Financial Damage after Cyberattack for Retailer i; $i=1,\dots,m$:

$$D_i p_i, \quad D_i \geq 0.$$

Expected Utility/Profit for Retailer $i, i=1,\dots,m$:

$$E(U_i)=(1-p_i)f_i(Q,s)+p_i(f_i(Q,s)-D_i)-h_i(s_i).$$

Utilities/Profits grouped into $E(U)$. Let K_i denote the feasible set corresponding to retailer i, where $K_i \equiv \{(Q_i,s_i)|Q_i \geq 0, \text{ and } 0 \leq s_i \leq 1\}$ and define $K \equiv \prod_{i=1}^{m} K_i$.

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

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

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

where

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

An equilibrium is established if no retailer can unilaterally improve upon his expected profits by selecting an alternative vector of product transactions and security levels.

Variational Inequality Formulation

Theorem 1: Variational Inequality Formulation of the Supply Chain Nash Equilibrium in Product Transactions and Security Levels

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

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

Variational Inequality Formulation

Theorem 1: Variational Inequality Formulation of the Supply Chain Nash Equilibrium in Product Transactions and Security Levels

Equivalently, $\forall (Q,s) \in K$,

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

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

Standard Variational Inequality Form

We put the previously discussed Nash equilibrium problem into a standard Variational Inequality form, that is: $X^* \in \mathcal{K} \subset R^N$, such that,

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

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

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,

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

the ith component, F^2_i, of $F^2(X)$ given by,

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

Qualitative Properties

Assumption

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

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

for all product transaction patterns Q with $Q_{ij} \geq M$. In other words, it is reasonable to assume that the expected utility of a seller would decrease whenever its product volume has become sufficiently large.

Qualitative Properties

Proposition 1: Existence of Equilibrium

Any supply chain Nash equilibrium problem in product transactions and security levels, as modeled above, that satisfies Assumption 1 possesses at least one equilibrium product transaction and security level pattern. The proof follows from Proposition 1 in Zhang and Nagurney (1995).

Proposition 2: Uniqueness of Equilibrium

Suppose that F is strictly monotone at any equilibrium point of the variational inequality problem. Then it has at most one equilibrium point.

The Algorithm

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

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

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

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

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

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

The Algorithm

Theorem 2: Convergence to a Unique Equilibrium under the Euler Method

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

Example Set 1

The first set of examples follows the following topology:

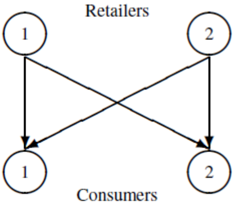

Fig. 2 Network Topology for Example Set 1

The cost functions for Example 1 are:

$$c_1 = 5; c_2 = 10; c_{11}(Q_{11}) = 0.5Q_{11}^2 + Q_{11}; c_{12}(Q_{12}) = 0.25Q_{12}^2 + Q_{12};$$

$c_{21}(Q_{21}) = 0.5Q_{21}^2 + 2; c_{22}(Q_{22}) = 0.25Q_{22}^2 + Q_{22}.$

The demand price functions are:

$$\rho_1(d_1, s) = -d_1 + 0.1(\frac{s_1 + s_2}{2}) + 100; \rho_2(d_2, s) = -5d_2 + 0.2(\frac{s_1 + s_2}{2}) + 200.$$

Example Set 1

The first set of examples follows the following topology:

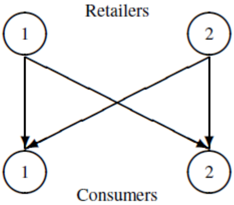

Fig. 2 Network Topology for Example Set 1

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

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

Hence, in Example 1 the vulnerability of Retailer 1 is .09 and that of Retailer 2 is also .09, with the network vulnerability being .09.

Example Set 1

In **Variant 1.1**, we change the demand price function of Consumer 1 to reflect an enhanced willingness to pay more for the product.

$$\rho_1(d_1, s) = -d_1 + 0.1(\frac{s_1 + s_2}{2}) + 200.$$

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

The vulnerability of Retailer 2 decreased slightly to 0.08.

Example Set 1

In **Variant 1.2**, Consumer 2 no longer values the product much. So, his demand price function is

$$\rho_2(d_2, s) = -0.5d_2 + 0.2(\frac{s_1 + s_2}{2}) + 20.$$

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

The vulnerability of Retailer 1 is now .12 and that of Retailer 2: .11 with the network vulnerability being: .115.

Example Set 1

In **Variant 1.3**, both security investment cost functions are increased so that:

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

and having new damages: $D_1 = 500$; $D_2 = 700$.

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

The vulnerability of Retailer 1 is now .34 and that of Retailer 2: .28 with the network vulnerability =.31.

Example Set 1

In **Variant 1.4**, Retailer 2's investment cost function is increased further so that:

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

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

The vulnerability of Retailer 1 is now: .27 and that of Retailer 2: .82. The network vulnerability for this example is: .54, the highest value in this set of examples.

Example Set 2

The second set of examples follows the following topology:

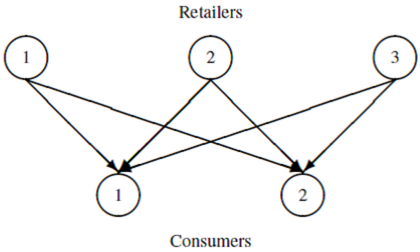

Fig. 3 Network Topology for Example Set 2

The cost functions for Example 2 are the same for Retailers 1 and 2. However, for the added Retailer 3:

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

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

Example Set 2

In **Variant 2.1**, we change the demand price function of Consumer 1 to reflect more sensitivity to network security.

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

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

Vulnerabilities of all firms have decreased.

Example Set 2

In **Variant 2.2**, Consumer 2 is also more sensitive to average security with a new demand price function given by:

$$\rho_2(d_2, s) = -0.5d_2 + (\frac{s_1 + s_2}{2}) + 200.$$

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

The vulnerability of Retailer 1,2 =.05, Retailer 3 = .14. The network vulnerability is .08.

Example Set 2

In **Variant 2.3**, we change the demand price functions:

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

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

The vulnerabilities of the Retailers 1,2 and 3 are: .07, 07, and .16 with the network vulnerability at .10.

Example Set 2

In **Variant 2.4**, we change the demand price functions:

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

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

Vulnerabilities of Retailers 1,2 and 3: .02, .02, and .05. Network vulnerability = .03.
This is the least vulnerable supply chain network.

Summary and Conclusions

- With companies seeking to determine how much they should invest in cybersecurity, **a general framework that can quantify the investments in cybersecurity in supply chain networks** is needed.

Summary and Conclusions

- With companies seeking to determine how much they should invest in cybersecurity, **a general framework that can quantify the investments in cybersecurity in supply chain networks** is needed.
- We derived the **variational inequality formulation** of the governing equilibrium conditions, discussed **qualitative properties**, and demonstrated that the **algorithm** is computationally effective.

Summary and Conclusions

- With companies seeking to determine how much they should invest in cybersecurity, **a general framework that can quantify the investments in cybersecurity in supply chain networks** is needed.
- We derived the **variational inequality formulation** of the governing equilibrium conditions, discussed **qualitative properties**, and demonstrated that the **algorithm** is computationally effective.
- The numerical results illustrated the impacts of an *increase in competition, changes in the demand price functions, changes in the damages incurred, and changes in the cybersecurity investment cost functions*.

Summary and Conclusions

- With companies seeking to determine how much they should invest in cybersecurity, **a general framework that can quantify the investments in cybersecurity in supply chain networks** is needed.
- We derived the **variational inequality formulation** of the governing equilibrium conditions, discussed **qualitative properties**, and demonstrated that the **algorithm** is computationally effective.
- The numerical results illustrated the impacts of an *increase in competition, changes in the demand price functions, changes in the damages incurred, and changes in the cybersecurity investment cost functions*.
- We also provide the vulnerability of each retailer and the **network vulnerability**.

Summary and Conclusions

- With companies seeking to determine how much they should invest in cybersecurity, **a general framework that can quantify the investments in cybersecurity in supply chain networks** is needed.
- We derived the **variational inequality formulation** of the governing equilibrium conditions, discussed **qualitative properties**, and demonstrated that the **algorithm** is computationally effective.
- The numerical results illustrated the impacts of an *increase in competition, changes in the demand price functions, changes in the damages incurred, and changes in the cybersecurity investment cost functions*.
- We also provide the vulnerability of each retailer and the **network vulnerability**.
- The approach of applying game theory and variational inequality theory with expected utilities to cybersecurity is unique.

Acknowledgements

- 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.

Thank You!

For more information, please visit:
http://supernet.isenberg.umass.edu/default.htm.