Topic 9: Cybercrime and Cybersecurity

Professor Anna Nagurney

John F. Smith Memorial Professor
Director – Virtual Center for Supernetworks
Isenberg School of Management
University of Massachusetts Amherst

SCH-MGMT 825 Management Science Seminar
Advances in Variational Inequalities, Networks, and Game Theory, Spring 2018

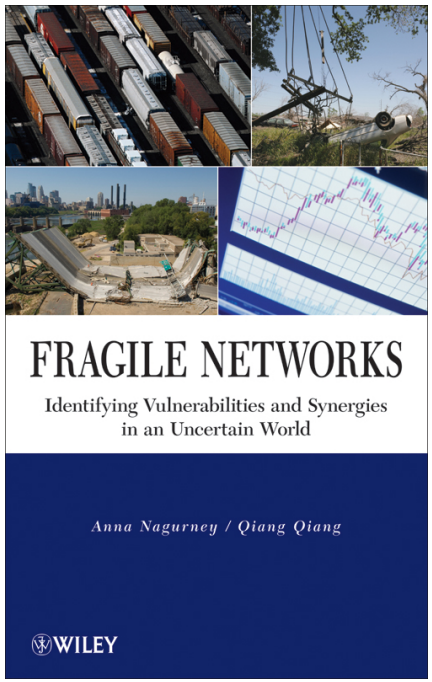
Outline

- Background and Motivation
- Which Nodes and Links Really Matter?
- Game Theory
- A Predictive Network Economic Model of Cybercrime
- Prescriptive Multifirm Models of Cybersecurity Investment: Competition vs. Cooperation
- Case Studies to the Retail and Energy Sectors
- Summary and Conclusions

Background and Motivation

How I Became Interested in Cybersecurity

One of my books, written with a UMass Amherst PhD alum, was "hacked" and digital copies of it posted on websites around the globe.



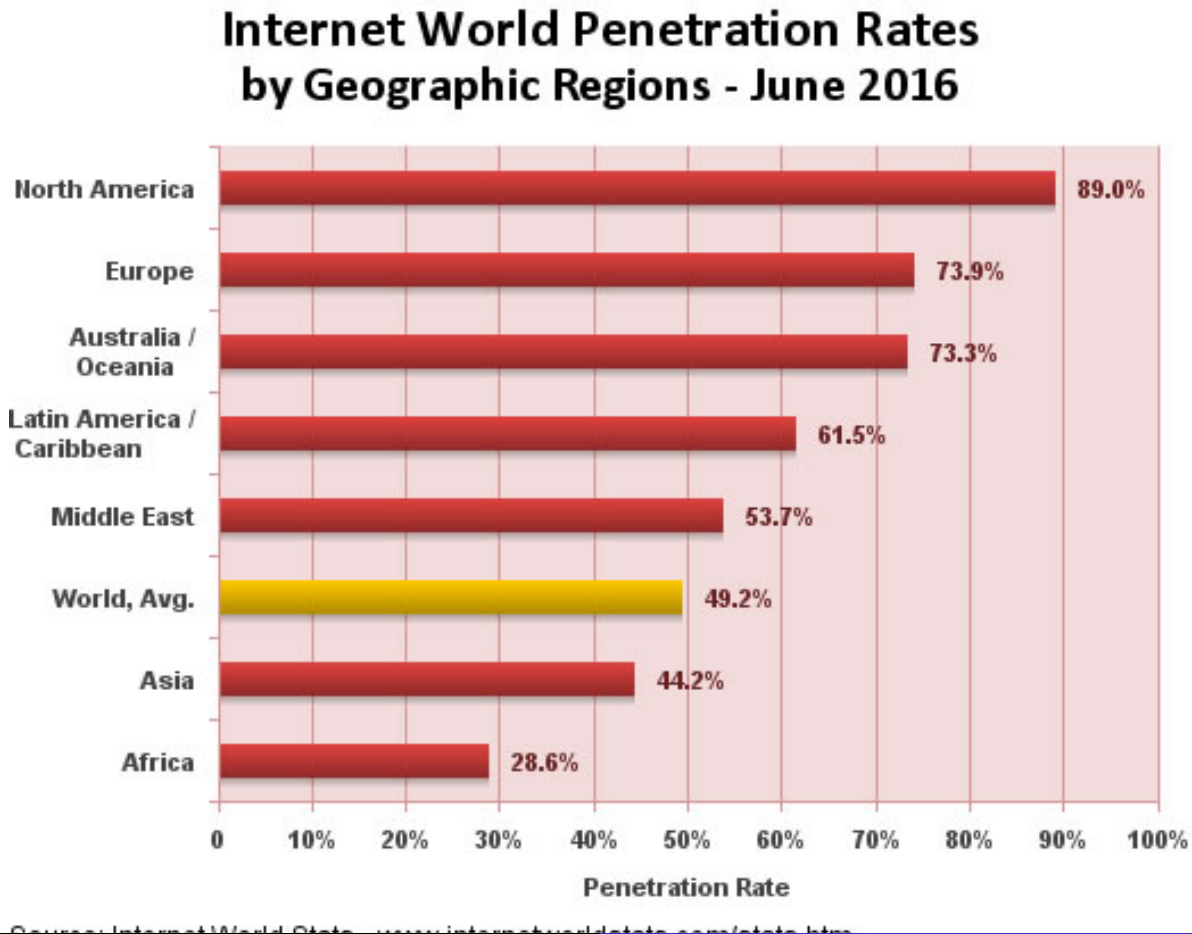
In a sense, this may be viewed as a compliment since clearly someone had determined that it has some sort of *value*.

The publisher John Wiley & Sons was notified and lawyers got involved but how do you contact and then influence those responsible for postings on rather anonymous websites?

About the same time news about cyberattacks was getting prominent attention in the media and there were those interested in working with us on related research on cybersecurity.

The Internet has transformed the ways in which individuals, groups, organizations communicate, obtain information, access entertainment, and conduct their economic and social activities.

In 2012, there were over 2.4 billion users. In 2016, there are 3.5 billion users, almost half of the world population



The Cost of Cybercrime

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.

Cybercrime

- **Cybercrimes are costly for organizations.**

All industries fall victim to cybercrime, but to different degrees with **defense, energy, and financial service companies** experiencing higher cybercrime costs than organizations in retail, hospitality, and consumer products.

Cybercrime

In 2014, 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 (The New York Times (2015)).

Since financial gains 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 (The Guardian (2015)) are some of the widely accepted cautionary tales in this sector.

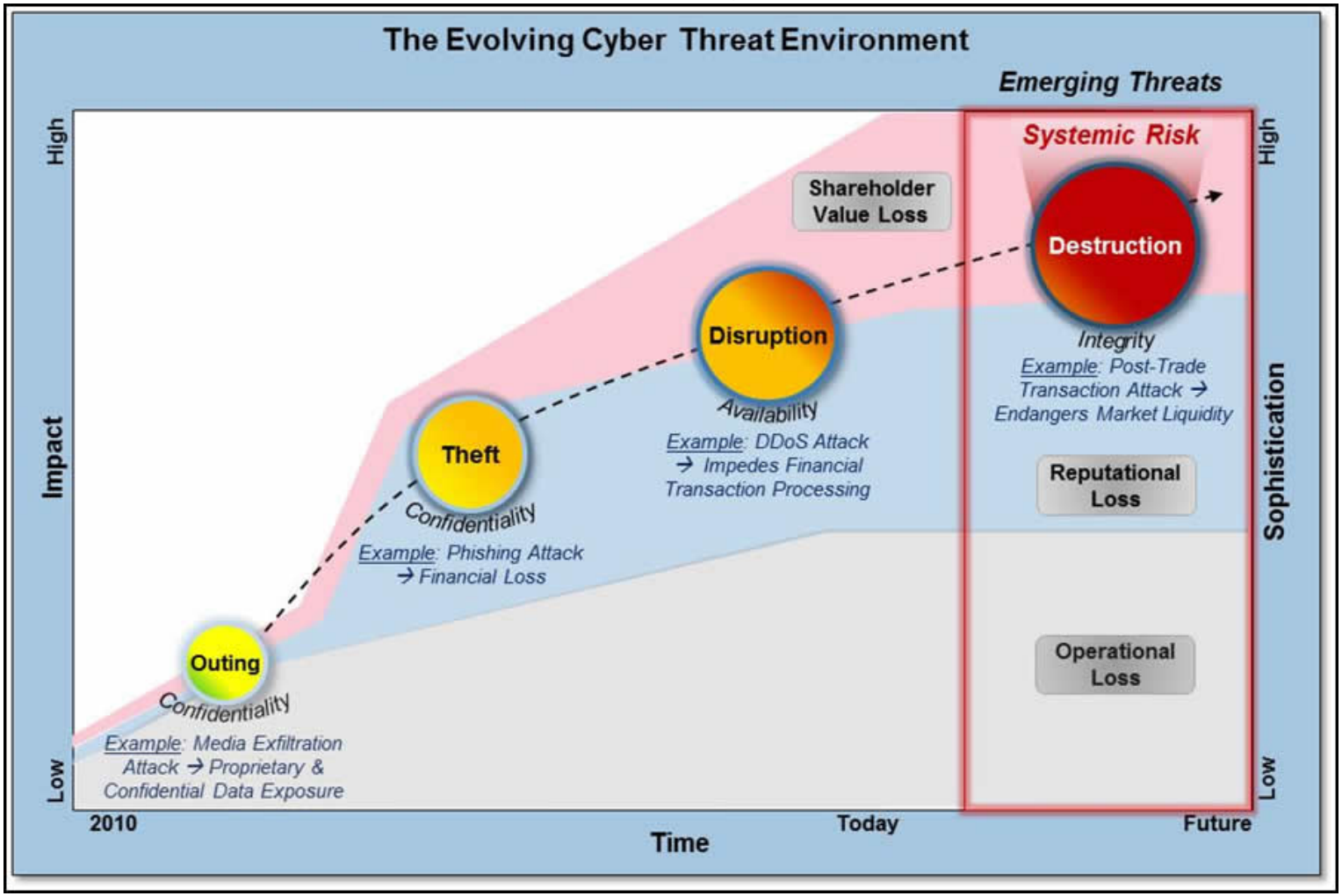
Cybercrime

More than 76 million households and seven million small businesses were compromised because of the JP Morgan attacks.

Clearly, hackers go where there is money.

The most costly cybercrimes (58% annually) are those caused by denial of service, malicious insider and web-based attacks.

Mitigation may require enabling technologies, intrusion prevention systems, applications security testing solutions and enterprise solutions.



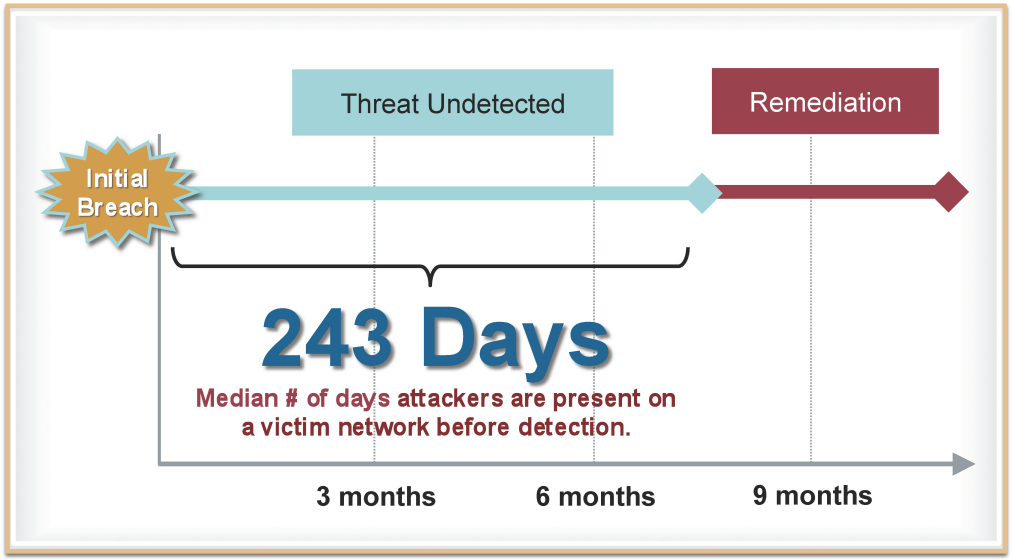
Source: Sarnowski for Booz Allen and Hamilton

Putting Cybercrime in Context

Putting Malicious Cyber Activity in Context			
CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Source: The Economic Impact of Cybercrime and Cyber Espionage, Center for Strategic and International Studies, July 2013, sponsored by McAfee.

Cyberattacks



Source: Mandiant M-Trends 2013

The median number of days that attackers were present on a victim's network before being discovered dropped to 146 days in 2015 from 205 days in 2014 – a trend that shows positive improvement since measuring 416 days back in 2012. However, breaches still often go undetected for years, according to Mandiant.

Cybercrime and Financial Institutions

According to a recent survey cybercrime is placing heavy strains on the global financial sector, with cybercrime now the second most commonly reported economic crime affecting financial services firms.

Cybercrime and Financial Institutions

According to a recent survey cybercrime is placing heavy strains on the global financial sector, with cybercrime now the second most commonly reported economic crime affecting financial services firms.

Cybercrime accounted for 38% of all economic crimes in the financial sector, as compared to an average of 16% across all other industries.

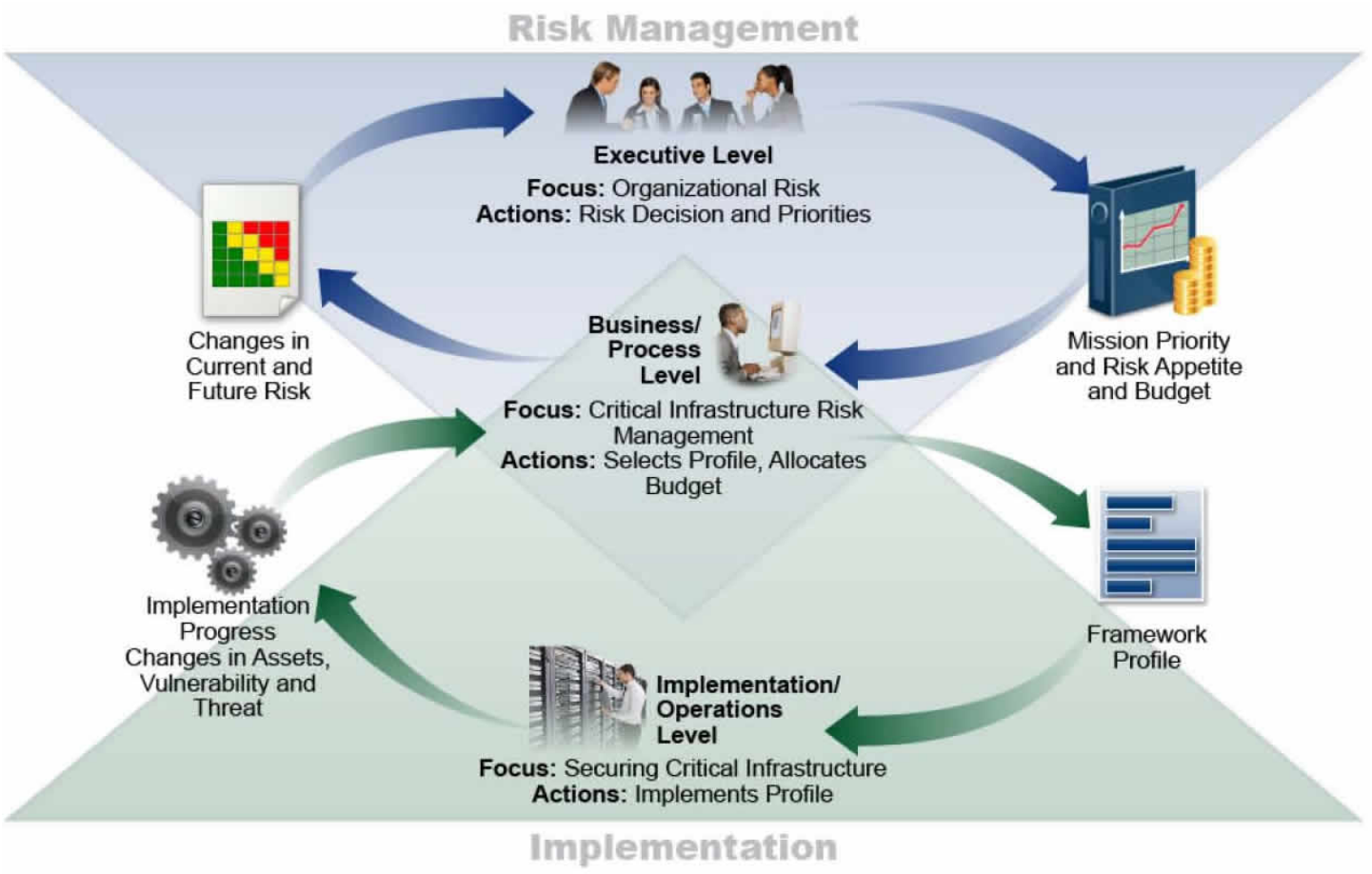
Cybercrime and Financial Institutions

According to a recent survey cybercrime is placing heavy strains on the global financial sector, with cybercrime now the second most commonly reported economic crime affecting financial services firms.

Cybercrime accounted for 38% of all economic crimes in the financial sector, as compared to an average of 16% across all other industries.

Cyberattacks are intrusive and economically costly. In addition, they may adversely affect a company's most valuable asset its reputation.

It's About Risk Management

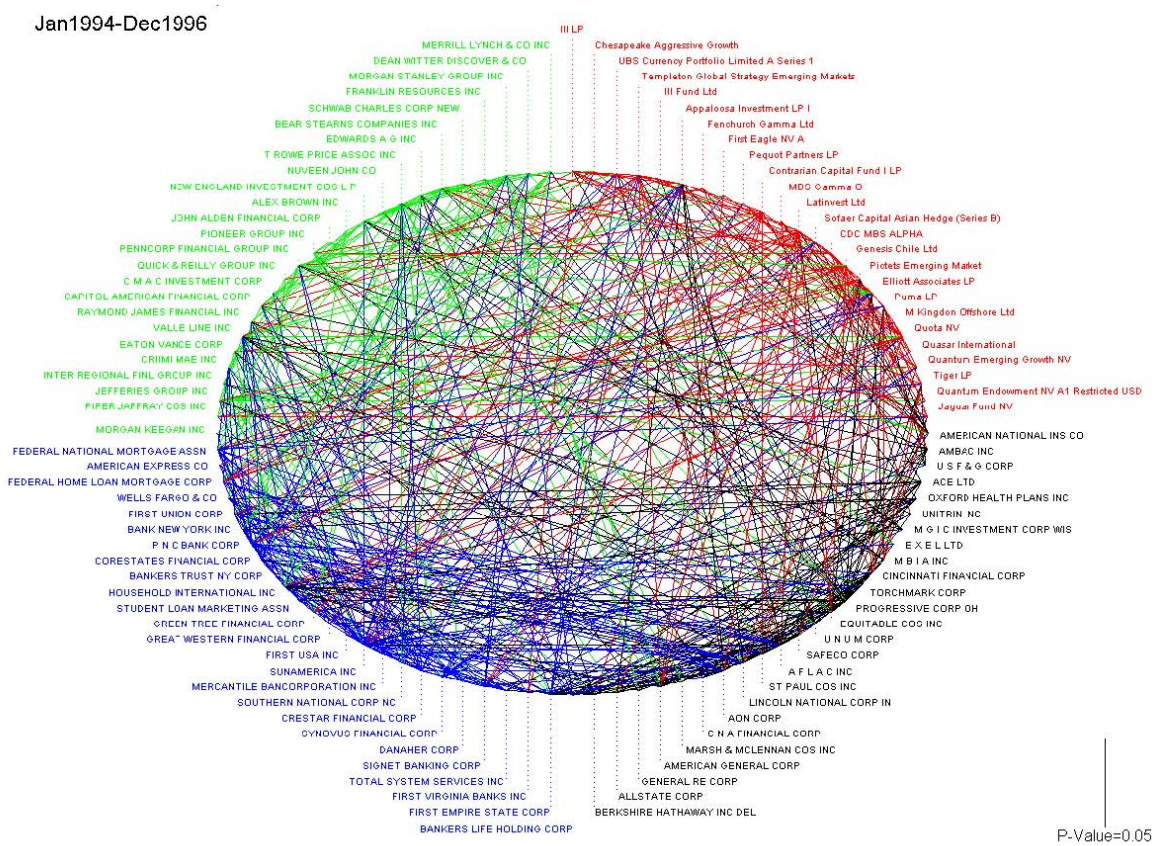


Source: Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), February 12, 2014

Our enterprises and organizations are critically dependent on infrastructure network systems including the Internet.

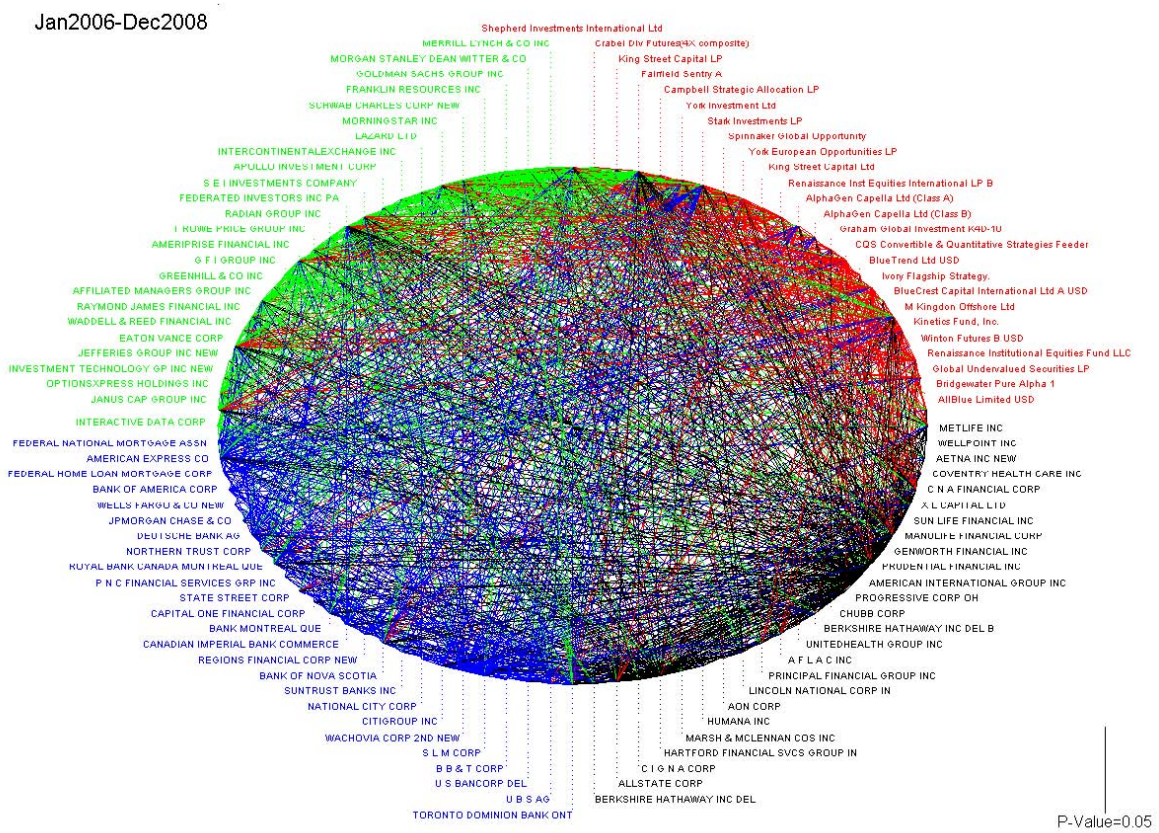
Which Nodes and Links Really Matter?

Empirical Evidence: Jan. 1994 - Dec. 1996 - Connectivity, Vulnerability



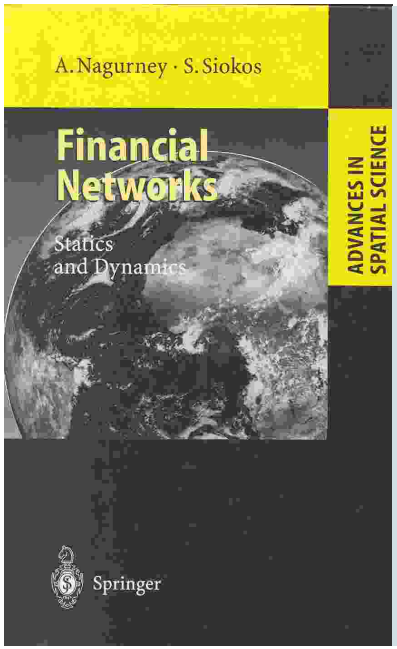
Granger Causality Results: **Green Broker**, **Red Hedge Fund**, Black Insurer, Blue Bank Source: Billio, Getmansky, Lo, and Pelizzon (2011)

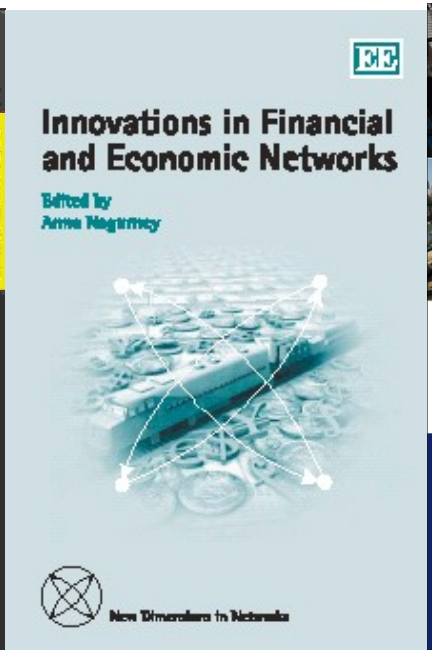
Empirical Evidence: Jan. 2006 - Dec. 2008 - Connectivity, Vulnerability

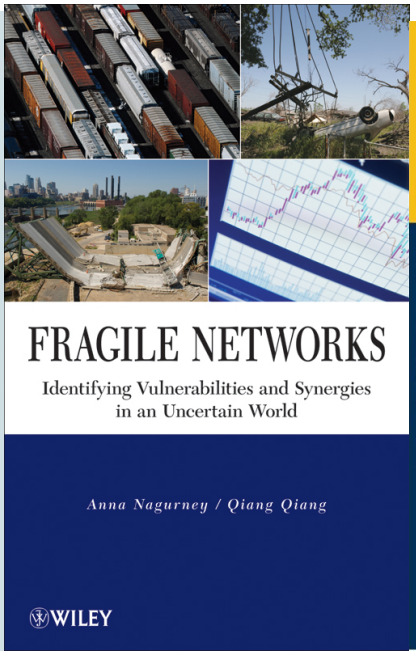


Granger Causality Results: **Green Broker**, **Red Hedge Fund**, Black Insurer, Blue Bank Source: Billio, Getmansky, Lo, and Pelizzon (2011)

Financial Networks and Game Theory

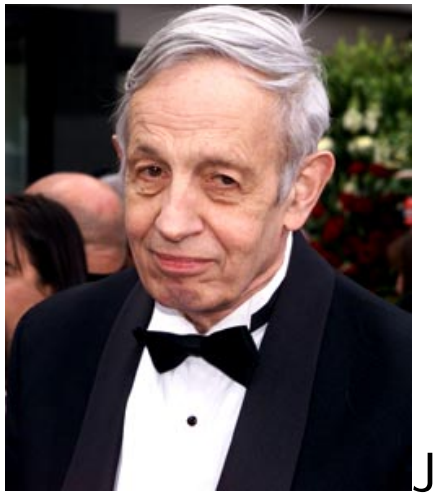






Game Theory

There are many game theory problems and tools for solving them. There is noncooperative game theory, in which the players or decision-makers compete with one anther, and cooperative game theory, in which players cooperate with one another.


John F. Nash

In **noncooperative games**, the governing concept is that of Nash equilibrium. In **cooperative games**, we can apply Nash bargaining theory.

A Predictive Network Economic Model of Cybercrime

Network Economics of Cybercrime

We lay the foundation for the development of network economics based models for cyberccrime in financial services.

Financial services firms as well as hackers are economic agents.

Our view is that financial firms produce/possess commodities (or products) that hackers (criminals) seek to obtain.

We assume that the firms (as well as the hackers) can be located in different regions of a country or in different countries. Financial service firms may also be interpreted as **prey** and the hackers as **predators**.

Network Economics of Cybercrime

Commodities or products that the hackers seek to acquire may include: credit card numbers, password information, specific documents, etc.

The financial firms are the producers of these commodities whereas the hackers act as agents and "sell" these products, if they acquire them, at the "going" market prices.

There is a "price" at which the hackers acquire the financial commodity from a financial institution and a price at which they sell the hacked product in the demand markets. The former we refer to as the supply price and the latter is the demand price.

Network Economics of Cybercrime

In addition, we assume that there is **a transaction cost associated between each pair of financial and demand markets for each commodity**. These transaction costs can be generalized costs that also capture risk.

Network Economics of Cybercrime

Indeed, if the cyber criminals do not find demand markets for their acquired financial commodities (since there are no consumers willing to pay the price) then there is no economic incentive for them to acquire the financial commodities.

Network Economics of Cybercrime

Indeed, if the cyber criminals do not find demand markets for their acquired financial commodities (since there are no consumers willing to pay the price) then there is no economic incentive for them to acquire the financial commodities.

To present another criminal network analogue – consider the market for illegal drugs, with the U.S. market being one of the largest, if not the largest one. If there is no demand for the drugs then the suppliers of illegal drugs cannot recover their costs of production and transaction and the flows of drugs will go to zero.

Network Economics of Cybercrime

Indeed, if the cyber criminals do not find demand markets for their acquired financial commodities (since there are no consumers willing to pay the price) then there is no economic incentive for them to acquire the financial commodities.

To present another criminal network analogue – consider the market for illegal drugs, with the U.S. market being one of the largest, if not the largest one. If there is no demand for the drugs then the suppliers of illegal drugs cannot recover their costs of production and transaction and the flows of drugs will go to zero. According to a recent Rand report, for many, the cyber black market can be more profitable than the illegal drug trade.

Network Economics of Cybercrime

• After the major Target breach, **some credit cards obtained thus initially sold for $135 each on the black market, but, within weeks, as banks started to cancel the cards, the price dropped to $8** and, seven months after Target learned about the breach, the cards had essentially no value.

• In addition, different brands of credit cards can be viewed as different products since they command different prices on the black market. For example, according to Leinwand Leger (2014) credit cards with the highest credit limits, such as an American Express Platinum card, command the highest prices.

Network Economics of Cybercrime

- A card number with a low limit might sell for \$1 or \$2, while a high limit card number can sell for \$15 or considerably more, as noted above. **Hacked credit card numbers of European credit cards can command prices five times higher than U.S. cards** (see Peterson (2013)).

Perishability and Cybercrime in Financial Products

There is a short time window during which the value of a financial product acquired through cybercrime is positive but it decreases during the time window. Hence, financial products such as credit cards that are hacked can be treated as perishable products such as fruits, vegetables, etc.

Perishability and Cybercrime in Financial Products

This part of the presentation is based on the paper, "A Multiproduct Network Economic Model of Cybercrime in Financial Services," Anna Nagurney, *Service Science*, **7(1)**, (2015) pp 70-81.

Perishability and Cybercrime in Financial Products

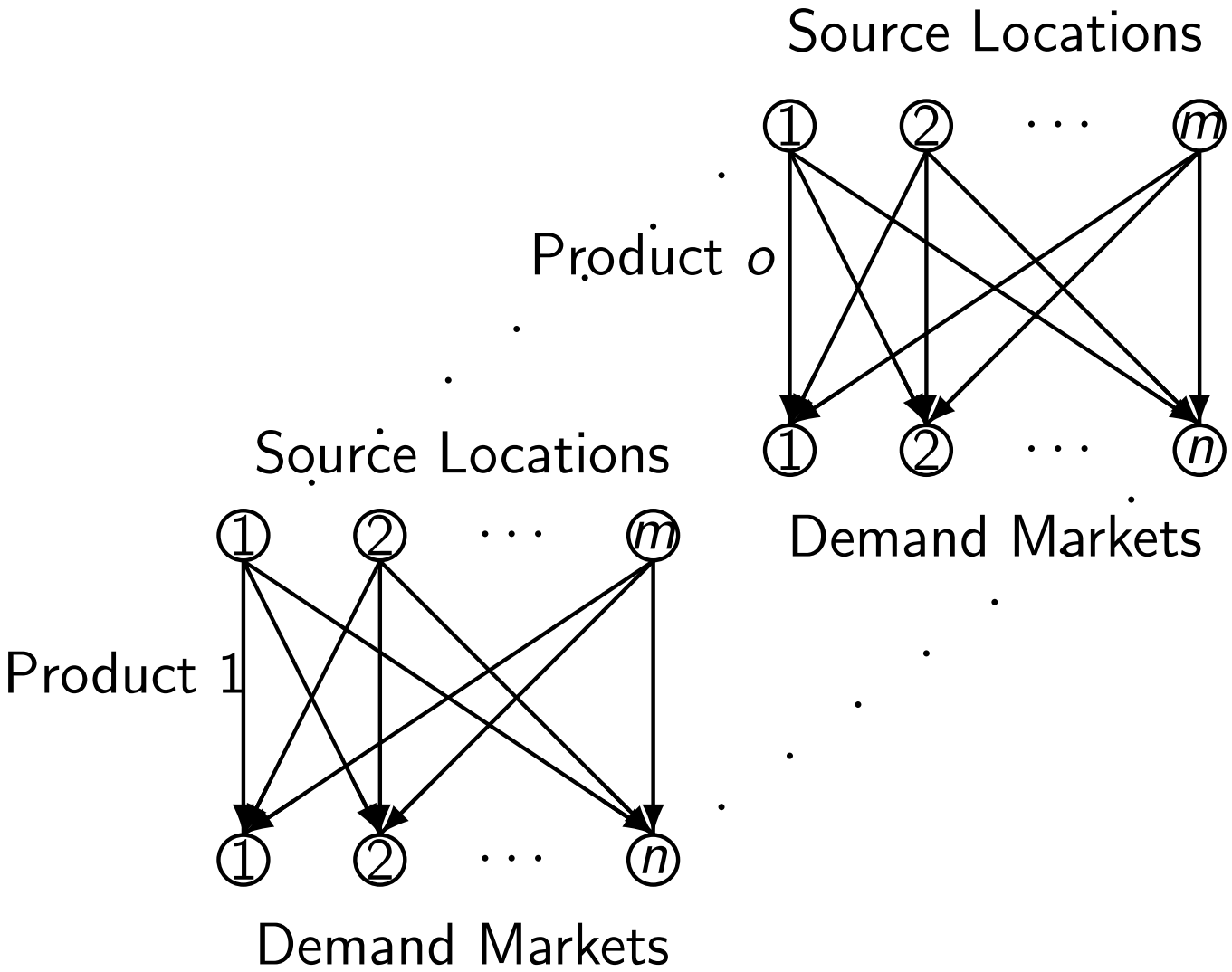


Figure: Structure of the Network Economic Problem

Some Notation - Variables

Let Q_{ij}^k denote the nonnegative amount of financial product k obtained from i and shipped to j. Q is the vector of Q_{ij}^ks.

Let s_i^k denote the nonnegative supply of financial product k at i and let d_j^k be the demand for k and j. s is the vector of s_i^ks and d is the vector of d_j^ks.

T_{ij}^k is the time between the acquisition of product k from source location i and its sale at j.

$T_{ave,j}^k$ is the average time for delivery of product k at demand market j, where $T_{ave,j}^k = \frac{\sum_{i=1}^m T_{ij}^k Q_{ij}^k}{d_j^k}$. T_{ave} is the vector of $T_{ave,j}^k$s.

Some Notation - Functions

Let $\pi_i^k(s)$ denote the price of acquiring product k at source location i.

Let $\rho_j^k(d, T_{ave})$ denote the demand price of financial product k at demand market j.

Let $\hat{c}_{ij}^k(Q)$ denote the unit transaction cost associated with transacting product k between i and j.

Conservation of Flow Equations

The conservation of flow equations are:

$$s_i^k = \sum_{j=1}^{n} Q_{ij}^k, \quad k = 1, \ldots, o; i = 1, \ldots, m,$$

$$d_j^k = \sum_{i=1}^{m} Q_{ij}^k, \quad k = 1, \ldots, o; i = 1, \ldots, n,$$

$$Q_{ij}^k \geq 0, \quad k = 1, \ldots, o; i = 1, \ldots, m; j = 1, \ldots, n.$$

In addition, we introduce the following expression, which captures time:

$$t_{ij}^k Q_{ij}^k + h_{ij}^k = T_{ij}^k, \quad k = 1, \ldots, o; i = 1, \ldots, m; j = 1, \ldots, n.$$

In view of the conservation of flow equations, we can define new demand price functions $\hat{\rho}_j^k$, $\forall k, \forall j$ as follows:

$$\hat{\rho}_j^k(Q) \equiv \rho_j^k(d, T_{ave}), \quad k = 1, \ldots, o; j = 1, \ldots, n.$$

If the demand at a demand market for a product is equal to zero, we remove that demand market from the network for that product since the corresponding time average would not be defined.

Also, we can define new supply price functions $\hat{\pi}_i^k$, $\forall k, \forall i$ as:

$$\hat{\pi}_i^k(Q) \equiv \pi_i^k(s), \quad k = 1, \ldots, o; j = 1, \ldots, n,$$

which allow us to construct a variational inequality formulation governing the equilibrium conditions below with nice features for computations. We assume that all the functions in the model are continuous.

The Network Economic Equilibrium Conditions

The network economic equilibrium conditions for cybercrime have been achieved if for all products k; $k = 1, \ldots, o$, and for all pairs of markets (i, j); $i = 1, \ldots, m$; $j = 1, \ldots, n$, the following conditions hold:

$$\hat{\pi}_i^k(Q^*) + c_{ij}^k(Q^*) \begin{cases} = \hat{\rho}_j^k(Q^*), & \text{if} \quad Q_{ij}^{k*} > 0 \\ \geq \rho_j^k(Q^*), & \text{if} \quad Q_{ij}^{k*} = 0, \end{cases}$$

where recall that $\hat{\pi}_i^k$ denotes the price of product k at source location i, c_{ij}^k denotes the unit transaction cost associated with k between (i, j), and $\hat{\rho}_j^k$ is the demand price of k at demand market j. Q_{ij}^{k*} is the equilibrium flow of product k between i and j with Q^* being the vector of all such flows.

We define the feasible set $K \equiv \{Q | Q \in R_+^{omn}\}$.

VI Formulation of the Equilibrium Conditions

Theorem: Variational Inequality Formulation

A product flow pattern $Q^* \in K$ is a cybercrime network economic equilibrium if and only if it satisfies the variational inequality problem:

$$\sum_{k=1}^{o}\sum_{i=1}^{m}\sum_{j=1}^{n}\left[\hat{\pi}_i^k(Q^*) + c_{ij}^k(Q^*) - \hat{\rho}_j^k(Q^*)\right]\times(Q_{ij}^k - Q_{ij}^{k*}) \geq 0, \forall Q \in K.$$

The above variational inequality problem can be put into standard form: determine $X^* \in \mathcal{K}$, such that

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

We define $\mathcal{K} \equiv K$, $X \equiv Q$, and $F(X) \equiv (F_{kij}(X))$; $k = 1, \ldots, o$; $i = 1, \ldots, m$; $j = 1, \ldots, n$, where $F_{kij} = \hat{\pi}_i^k(Q) + c_{ij}^k(Q) - \hat{\rho}_j^k(Q)$.

The Algorithm

The Euler Method

At each iteration τ one solves the following problem:

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

where $P_{\mathcal{K}}$ is the projection operator.

As shown in Dupuis and Nagurney (1993) and Nagurney and Zhang (1996), for convergence of the general iterative scheme, which induces the Euler method, among other methods, the sequence $\{a_{\tau}\}$ must satisfy: $\sum_{\tau=0}^{\infty} a_{\tau} = \infty$, $a_{\tau} > 0$, $a_{\tau} \rightarrow 0$, as $\tau \rightarrow \infty$.

Explicit Formulae

In particular, we have the following closed form expression for the product flows $k = 1, \ldots, m$; $i = 1, \ldots, m$; $j = 1, \ldots, n$:

$$Q_{ij}^{k\,\tau+1} = \max\{0, Q_{ij}^{k\,\tau} + a_{\tau}(\hat{\rho}_j^k(Q^{\tau}) - c_{ij}^k(Q^{\tau}) - \hat{\pi}_i^k(Q^{\tau})\}.$$

Numerical Examples: 2 Financial Products, 2 Supply Markets, and 2 Demand Markets

The network topology of the examples is as in Figure 3.

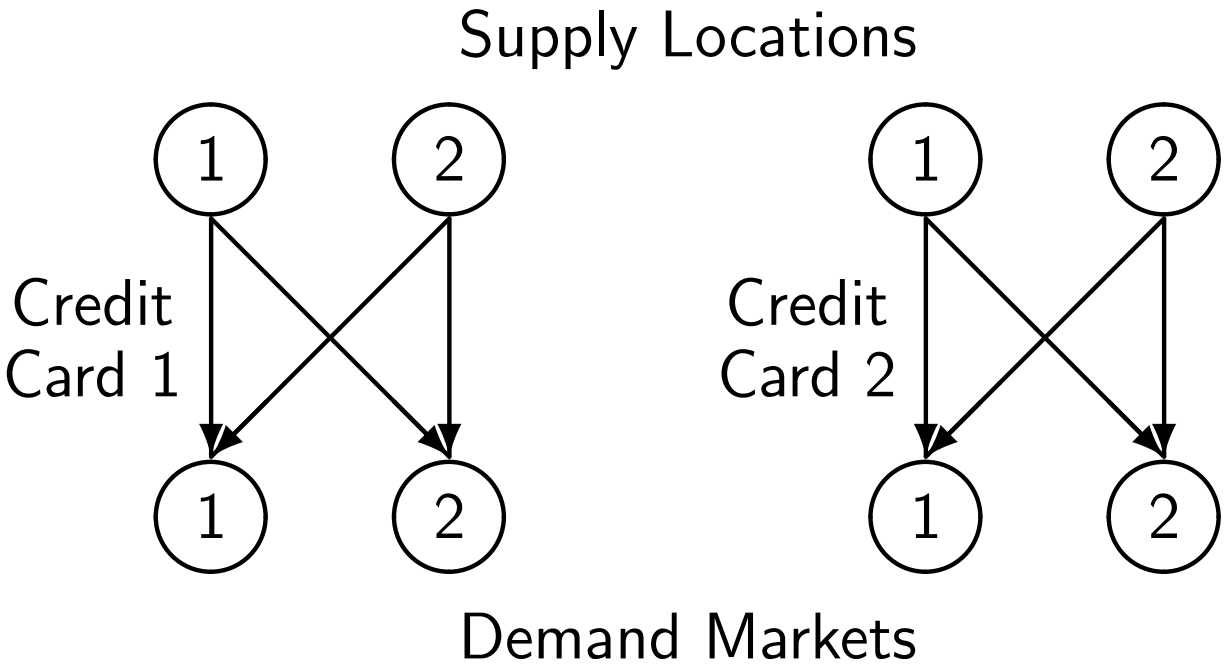


Figure: Topology of Examples

Numerical Examples: 2 Financial Products, 2 Supply Markets, and 2 Demand Markets

Example 1

The supply price functions are:

$$\pi_1^1(s) = 5s_1^1 + s_2^1 + 2, \quad \pi_2^1(s) = 2s_2^1 + s_1^1 + 1,$$

$$\pi_1^2(s) = 2s_1^2 + s_1^1 + 1, \quad \pi_2^2(s) = s_2^2 + .5s_2^1 + 1.$$

The unit transaction cost functions are:

$$c_{11}^1(Q) = .03{Q_{11}^1}^2 + 3Q_{11}^1 + 1, \quad c_{21}^1(Q) = .02{Q_{21}^1}^2 + 2Q_{21}^1 + 2,$$

$$c_{11}^2(Q) = .01{Q_{11}^2}^2 + Q_{11}^2 + 1, \quad c_{21}^2(Q) = .001{Q_{21}^2}^2 + .1Q_{21}^2 + 1,$$

$$c_{12}^1(Q) = .01{Q_{12}^1}^2 + Q_{12}^1 + 1, \quad c_{22}^1(Q) = .01{Q_{22}^1}^2 + Q_{22}^1 + 1,$$

$$c_{12}^2(Q) = .01{Q_{12}^2}^2 + Q_{12}^2 + 1, \quad c_{22}^2(Q) = .02{Q_{22}^2}^2 + 2Q_{22}^2 + 2.$$

Numerical Examples: 2 Financial Products, 2 Supply Markets, and 2 Demand Markets

Example 1

The demand price functions are:

$$\rho_1^1(d, T_{ave}) = -2d_1^1 - d_1^2 - .5\,T_{ave,1}^1 + 500,$$

$$\rho_1^2(d) = -3d_1^2 - d_1^1 - .1\,T_{ave,1}^2 + 300,$$

$$\rho_2^1(d, T_{ave}) = -d_2^1 - .5d_2^2 - .2\,T_{ave,2}^1 + 200,$$

$$\rho_2^2(d, T_{ave}) = -2d_2^2 - d_2^1 - .1\,T_{ave,2}^2 + 100.$$

Numerical Examples: 2 Financial Products, 2 Supply Markets, and 2 Demand Markets

Example 1 The time expressions are:

$$T_{11}^1 = .1Q_{11}^1 + 10, \quad T_{21}^1 = .5Q_{21}^1 + 5,$$
$$T_{11}^2 = .1Q_{11}^2 + 20, \quad T_{21}^2 = .5Q_{21}^2 + 15,$$
$$T_{12}^1 = .1Q_{12}^1 + 10, \quad T_{22}^1 = .1Q_{22}^1 + 10,$$
$$T_{12}^2 = .5Q_{12}^2 + 5, \quad T_{22}^2 = .5Q_{22}^2 + 10,$$

so that

$$T_{ave,1}^1 = \frac{T_{11}^1 Q_{11}^1 + T_{21}^1 Q_{21}^1}{d_1^1}, \quad T_{ave,1}^2 = \frac{T_{11}^2 Q_{11}^2 + T_{21}^2 Q_{21}^2}{d_1^2}.$$

$$T_{ave,2}^1 = \frac{T_{12}^1 Q_{12}^1 + T_{22}^1 Q_{22}^1}{d_2^1}, \quad T_{ave,2}^2 = \frac{T_{12}^2 Q_{12}^2 + T_{22}^2 Q_{22}^2}{d_2^2}.$$

The Euler method converged to the solution reported in Tables 1 and 2.

Example 2

Example 2

Example 2 has the same data as Example 1 except that now we have a modification in the demand price function associated with the second product at demand market 2 so that:

$$\rho_2^2(d, T_{ave}) = -2d_2^2 - d_2^1 - .1T_{ave,2}^2 + 200.$$

Such a change might represent that the value of this financial product has increased at that demand market.

Example 3

Example 3

Example 3 was constructed from Example 2 and had the same data except that we increased the fixed terms in all the transaction cost functions so that:

$$c_1^1(Q) = .03{Q_{11}^1}^2 + 3Q_{11}^1 + 10, \quad c_{21}^1(Q) = .02{Q_{21}^1}^2 + 2Q_{21}^1 + 20,$$

$$c_{11}^2(Q) = .01{Q_{11}^2}^2 + Q_{11}^2 + 10, \quad c_{21}^1(Q) = .001{Q_{21}^2}^2 + .1Q_{21}^2 + 10,$$

$$c_{12}^1(Q) = .01{Q_{12}^1}^2 + Q_{12}^1 + 10, \quad c_{22}^1(Q) = .01{Q_{22}^1}^2 + Q_{22}^1 + 10,$$

$$c_{12}^2(Q) = .01{Q_{12}^2}^2 + Q_{12}^2 + 10, \quad c_{22}^2(Q) = .02{Q_{22}^2}^2 + 2Q_{22}^2 + 20.$$

This could represent the situation that the cybercriminals have a harder time fencing all the products at all the demand markets. The results are reported in Tables 1 and 2.

Results

Table: Equilibrium Solutions for the Examples

Financial Flows	Example 1	Example 2	Example 3
$Q_{11}^{1}{}^{*}$	25.93	26.31	26.21
$Q_{12}^{1}{}^{*}$	0.00	0.00	0.00
$Q_{21}^{1}{}^{*}$	46.73	48.28	46.45
$Q_{22}^{1}{}^{*}$	16.77	12.50	11.61
$Q_{11}^{2}{}^{*}$	11.69	4.81	3.47
$Q_{12}^{2}{}^{*}$	6.09	23.46	23.59
$Q_{21}^{2}{}^{*}$	37.56	39.27	39.57
$Q_{22}^{2}{}^{*}$	0.00	12.67	9.69

Results

Table: Incurred Equilibrium Prices and Average Times

Prices	**Example 1**	**Example 2**	**Example 3**
$\rho_1^1(d^*, T_{ave}^*)$	294.07	295.07	300.35
$\rho_1^2(d^*, T_{ave}^*)$	76.52	89.85	94.87
$\rho_2^1(d^*, T_{ave}^*)$	175.51	164.94	167.28
$\rho_2^2(d^*, T_{ave}^*)$	69.98	113.86	120.52
Average Times	**Example 1**	**Example 2**	**Example 3**
$T_{ave,1}^1$	22.74	23.32	22.59
$T_{ave,1}^2$	30.78	33.09	33.62
$T_{ave,2}^1$	23.35	22.50	22.32
$T_{ave,2}^2$	10.61	13.75	13.08

Managerial Insights

- The above numerical examples, although stylized, provide important managerial insights that cybersecurity professionals may take advantage of in securing their data.

Managerial Insights

• The above numerical examples, although stylized, provide important managerial insights that cybersecurity professionals may take advantage of in securing their data.

• The examples show the quantified impacts of changes in the data on the equilibrium financial product flows, and on the incurred demand prices and average times for product delivery.

Managerial Insights

• The above numerical examples, although stylized, provide important managerial insights that cybersecurity professionals may take advantage of in securing their data.

• The examples show the quantified impacts of changes in the data on the equilibrium financial product flows, and on the incurred demand prices and average times for product delivery.

• The results are consistent with existing data on hacked credit cards. **Goncharov (2012) reports that the cost, that is, the supply price, of hacking into various accounts can range anywhere from $16 to over $325. Ablon, Libicki, and Golay (2014), note that, following an initial breach, the markets may get flooded with cybercrime products leading to a decrease in prices, which the structure of our demand price functions capture.**

Managerial Insights

• Credit cards acquired in the Target breach **initially fetched from $20 to $135 depending on the type of card, expiration date as well as limit (cf. Ablon, Libicki, and Golay (2014))**. Although our numerical study did not focus on a specific historical data breach, the results are not inconsistent with results obtained in practice.

Managerial Insights

• Credit cards acquired in the Target breach **initially fetched from $20 to $135 depending on the type of card, expiration date as well as limit (cf. Ablon, Libicki, and Golay (2014))**. Although our numerical study did not focus on a specific historical data breach, the results are not inconsistent with results obtained in practice.

• Finally, the model captures the crucial time element in the demand market pricing of products obtained through cybercrime with a focus on financial services.

Prescriptive Multifirm Models of Cybersecurity Investment Competition vs. Cooperation

Multifirm Models of Cybersecurity Investment

This part of the presentation is based on the paper, "Multifirm Models of Cybersecurity Investment Competition vs. Cooperation and Network Vulnerability," Anna Nagurney and Shivani Shukla, *European Journal of Operational Research*, in press, where many references and additional theoretical and numerical results can be found.

Investing in Cybersecurity

There is a growing interest in developing rigorous frameworks for cybersecurity investments.

As reported in Morgan (2016), **JPMorgan doubled its cybersecurity spending in 2015 to $500 million from $250 million previously**.

Gartner predicts that **worldwide spending on information security products and services will reach $81.6 billion in 2016 – an increase of 7.9% from last year**.

It is clear that making the best cybersecurity investments is a very timely problem and issue.

Common Features of the Models

We describe three different models of multifirm cybersecurity investments.

The first model is a Nash Equilibrium (NE) one capturing noncooperative behavior; the second and third are cooperative models, using Nash Bargaining (NB) and System-Optimization (S-O) concepts, respectively.

Common Features of the Models

There are m firms in the "network." These firms can be financial service firms, energy firms, manufacturing firms, or even retailers.

Each firm i; $i = 1, \ldots, m$, 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, wlog, by s_i; $i = 1 \ldots, m$.

Common Features of the Models

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

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

where $u_{s_i} < 1$, and is also greater than zero, is the upper bound on the security level for firm i.

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.

Common Features of the Models

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.

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

$$h_i(s_i) = \alpha_i\left(\frac{1}{\sqrt{(1 - s_i)}} - 1\right)$$

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).

Common Features of the Models

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

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

The vulnerability of firm i, $v_i = (1 - s_i)$, and the network vulnerability, $\bar{v} = (1 - \bar{s})$.

Common Features of the Models

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

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

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.

Common Features of the Models

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 is $\sqrt{W_i}$ (see Shetty et al. (2009)).

Also, a firm i is faced with damage D_i if there is a successful cyberattack on it.

Common Features of the Models

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

$$E(U_i) = (1 - p_i)f_i(W_i) + p_i(f_i(W_i - D_i)) - h_i(s_i).$$

We may write $E(U_i) = E(U_i(s)), \forall i$. Each $E(U_i(s))$ is strictly concave with respect to s_i under the assumed functional forms above since we also know that each $h_i(s_i)$; $i = 1, \ldots, m$ is strictly convex.

The Nash Equilibrium Model

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. 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.

Definition: 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 $i; i = 1, \ldots, m$:

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

where

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

VI Formulation of the NE Model

Theorem: Variational Inequality Formulation of Nash Equilibrium in Cybersecurity Levels

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

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

or the VI

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

Algorithm for the Solution of the NE Model

We can apply the Euler method, presented earlier to solve this model

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:

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

$$\max\{0, \min\{u_{s_i}, s_i^\tau + a_\tau(-\frac{\partial h_i(s_i^\tau)}{\partial s_i^\tau} - (f_i(W_i) - f_i(W_i - D_i))$$

$$\left[\frac{1}{m}\sum_{j=1}^{m} s_j^\tau - 1 - \frac{1}{m} + \frac{s_i^\tau}{m}\right]\}\}.$$

The Nash Bargaining Model

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). An excellent overview can be found in Binmore, Rubinstein, and Wolinsky (1989) and in the book by Muthoo (1999).

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

The Nash Bargaining Model

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

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

The optimization problem to be solved is then:

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

subject to:

$$E(U_j(s)) \geq E(U_j^{NE}), \quad j = 1, \ldots, m,$$

$$s \in K^1.$$

We define the feasible set K^2 consisting of the above constraints, which we know is convex.

The System-Optimization Model

Under system-optimization, the objective function becomes:

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

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:

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

subject to:

$$s \in K^1.$$

Numerical Case Studies

Solutions of the Nash Equilibrium model were computed by applying the Euler method, 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 $u_{s_i} = 0.99, \forall i$.

Numerical Case Studies

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.

A Retail Case Study

A Retail Case Study

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.

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 Newsweek (2014).

A Retail Case Study

Firm 2 represents 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 (Newsweek (2014)).

Firm 1 (Target) suffered $148 million in damages, according to the Consumer Bankers Association and the Credit Union National Association (Newsweek (2014)). Firm 2 (Home Depot) incurred a $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 (Newsweek (2014)).

A Retail Case Study

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): $D_1 = 148.0$; $D_2 = 152$.

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:

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

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

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

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

Results

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.

Sensitivity Analysis

We report the results for sensitivity analysis by increasing the values of the D_i parameters for $i = 1, 2$. The wealth and alpha parameters are fixed as previously: (in US$ in millions) $W_1 = 72600$, $W_2 = 78800$ (in millions); $\alpha_1 = 0.25$, $\alpha_2 = 0.30$. The solutions are reported in the following Tables.

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	268.476	279.648	268.485	279.658	268.484	279.659
34800	35200	268.377	279.542	268.386	279.551	268.385	279.552
44800	45200	268.290	279.451	268.300	279.461	268.300	279.461

Table: Expected Utilities for NE, NB, and S-O for Target and Home Depot for Varying D_i Parameters for $\alpha_1 = .25$ and $\alpha_2 = .30$

Sensitivity Analysis

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	.924	.915	.08040	.933	.924	.07165	.933	.924	.07166
34800	35200	.935	.927	.06890	.943	.935	.06144	.943	.934	.06145
44800	45200	.943	.935	.06090	.949	.942	.05431	.949	.942	.05432

Table: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for Target and Home Depot for Varying D_i Parameters for $\alpha_1 = .25$ and $\alpha_2 = .30$

Sensitivity Analysis

The network vulnerability is consistently the lowest under the NB solution concept, demonstrating the benefit of bargaining for cooperation in cybersecurity. The increase in expected utilities on employing NB over NE is US$ 10,193 for Target and US$ 10,346 for Home Depot in the scenario with $D_1 = 44800$, $D_2 = 45200$. Comparison of S-O and NB shows an increase of US$ 515 for Home Depot but a decrease of US$ 513 for Target when $D_1 = 44800$, $D_2 = 45200$.

Additional Sensitivity Analysis

We now report the results for additional sensitivity analysis by increasing the values of the D_i parameters for $i = 1, 2$, where the wealth and alpha parameters as follows: (in US$ in millions): $W_1 = 72600$, $W_2 = 78800$ (in millions); $\alpha_1 = 100.00$, $\alpha_2 = 120.00$. The results are reported in the subsequent Tables. The higher alpha parameters result in a significant increase in expected utilities as we move from NE to NB and S-O.

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: Expected Utilities for NE, NB, and S-O for Target and Home Depot for Varying D_i Parameters for $\alpha_1 = 100.00$ and $\alpha_2 = 120.00$

Additional Sensitivity Analysis

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: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for Target and Home Depot for Varying D_i Parameters $\alpha_1 = 100.00$ and $\alpha_2 = 120.00$

Additional Sensitivity Analysis

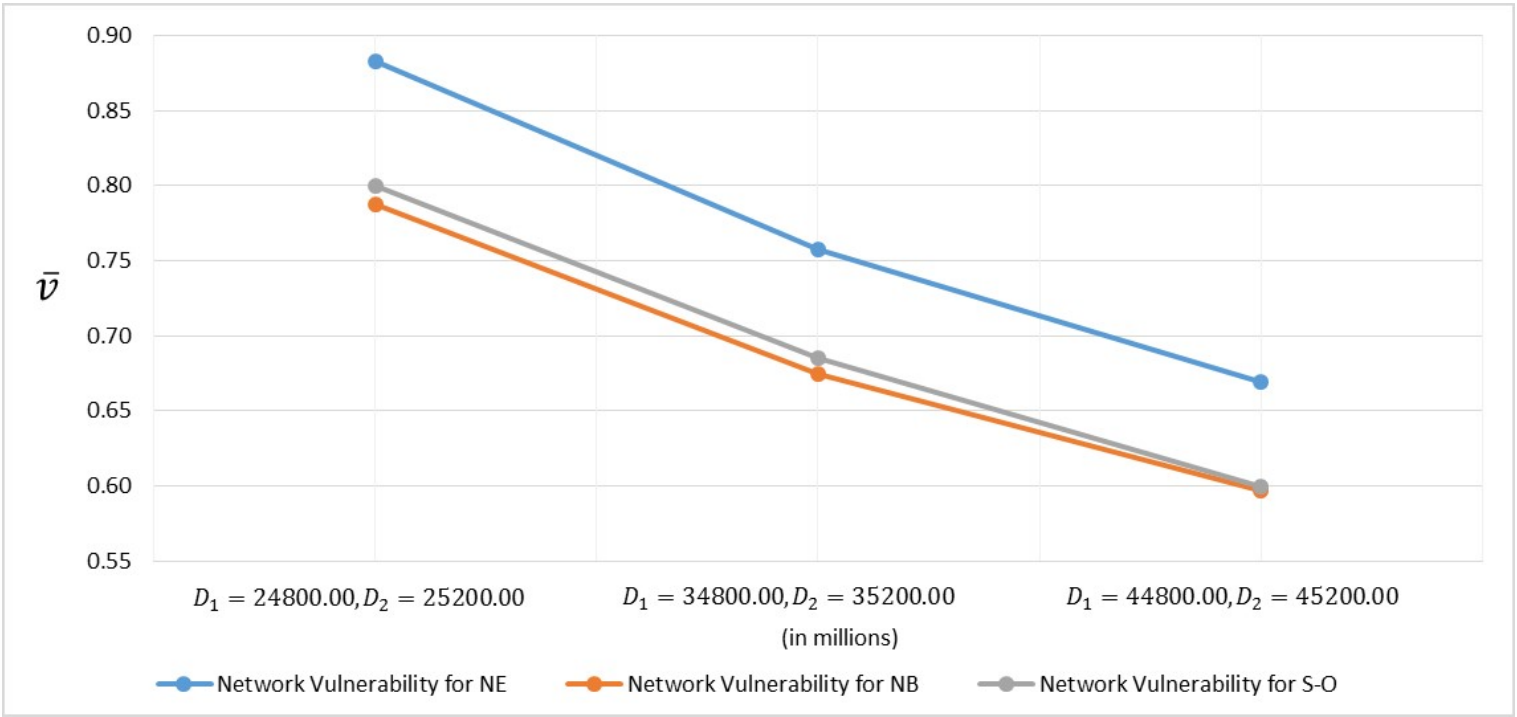


Figure: Representation of Table Showing Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O with Varying D_i Parameters $\alpha_1 = 100.00$ and $\alpha_2 = 120.00$

Additional Sensitivity Analysis

The network vulnerability is consistently the lowest for the NB solution, signifying the benefits of cooperation for cybersecurity.

An Energy Case Study

An Energy Case Study

Cyber espionage assaults targeting the energy sector have seen a sharp rise since 2007. Increases in automation and dependency on technology have led to many more vulnerabilities in this sector than the companies envisioned. One such attack on some of the major players in the industry by the Chinese is called Night Dragon.

The attack persisted for more than a few years before being detected in 2011. Proprietary information about oil and gas field operations, related financial transactions, exploratory maps, bidding data, and other sensitive information was compromised (OffShore Engineer (2013)).

The losses emanating from such an assault can be catastrophic.

An Energy Case Study

In this case study, we consider three internationally renowned oil and gas companies.

Firm 1 represents Royal Dutch Shell Plc, an Anglo-Dutch multinational company with operations spanning worldwide. Its sales and revenue make it the third largest in the world.

Firm 2 is British Petroleum (BP) in this case study. The company is the seventh largest in terms of its turnover and is headquartered in the UK.

Firm 3 is Exxon Mobil, the largest oil and gas company in the US and the fourth largest in the world. All of these firms were victims of the Night Dragon attack and suffered critical loss of information.

An Energy Case Study

In millions, we let $W_1 = 293290$; $W_2 = 234250$; $W_3 = 437640$. The information that was compromised provided important details such as possible points of exploration, current status, future plans, etc.

Since the actual damage was confidential and not reported, we have estimated it by multiplying the throughput of each of these firms (barrels produced per day for six months) with the oil price of \$53.5. As of 2014, the daily production of Shell was 3.9 million barrels, that of BP was 4.1 million barrels, and that of Exxon Mobil was 5.3 million barrels (Statista (2015)).

An Energy Case Study

We added the average costs of detection and escalation, notification and ex-post response for UK (BP and Shell) and US (Exxon Mobil). The averages were obtained from the Ponemon Institute study (2013).

Thus, the potential damages these firms could stand to sustain, from a similar cyberattack to the above, amount to (in millions): $D_1 = 38080.4$; $D_2 = 40033.1$; $D_3 = 51750.3$. These are approximate values only.

An Energy Case Study

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:

$$h_1(s_1) = 0.094\left(\frac{1}{\sqrt{1 - s_1}} - 1\right); \quad h_2(s_2) = 0.075\left(\frac{1}{\sqrt{1 - s_2}} - 1\right);$$

$$h_1(s_3) = 0.085\left(\frac{1}{\sqrt{1 - s_3}} - 1\right).$$

The α_i; $i = 1, 2, 3$, values in the cybersecurity investment cost functions above represent the total number of employees of the organizations in millions.

Results

Solution	NE	NB	S-O
s_1	0.936	0.945	0.946
s_2	0.949	0.957	0.956
s_3	0.943	0.951	0.951
v_1	0.064	0.055	0.054
v_2	0.051	0.043	0.044
v_3	0.057	0.049	0.049
$\bar{s}$	0.942	0.951	0.951
$\bar{v}$	0.058	0.049	0.049
$E(U_1)$	541.151	541.157	541.156
$E(U_2)$	483.609	483.615	483.617
$E(U_3)$	661.142	661.150	661.149

Table: Results for NE, NB, and S-O for Shell, BP, and Exxon Mobil

Results

Similar to the first case study based on retailers, we observe that, in the results for the Nash Bargaining model, the security levels of all three firms are higher as compared to their respective values in the Nash Equilibrium model.

Once again, the Nash Bargaining solution manages the security of the network and the monetary expectations well for all three firms, benefiting the network and the consumers.

Sharing of cyber information among these companies could be tricky, yet, nevertheless, essential.

LOGIIC, Linking the Oil and Gas Industry to Improve Cybersecurity, was established for collaboration among companies in this sector and the US Department of Homeland Security. BP, Chevron, Shell, Total and others possessing global energy infrastructure are members of the program (Automation Federation (2013)).

Based on these case studies, which describe results for different industrial sectors, 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.

Cybersecurity and Supply Chains

Figure: Supply chains are also vulnerable to cyber attacks and can serve as entre points

Cybersecurity, Supply Chains, and Game Theory

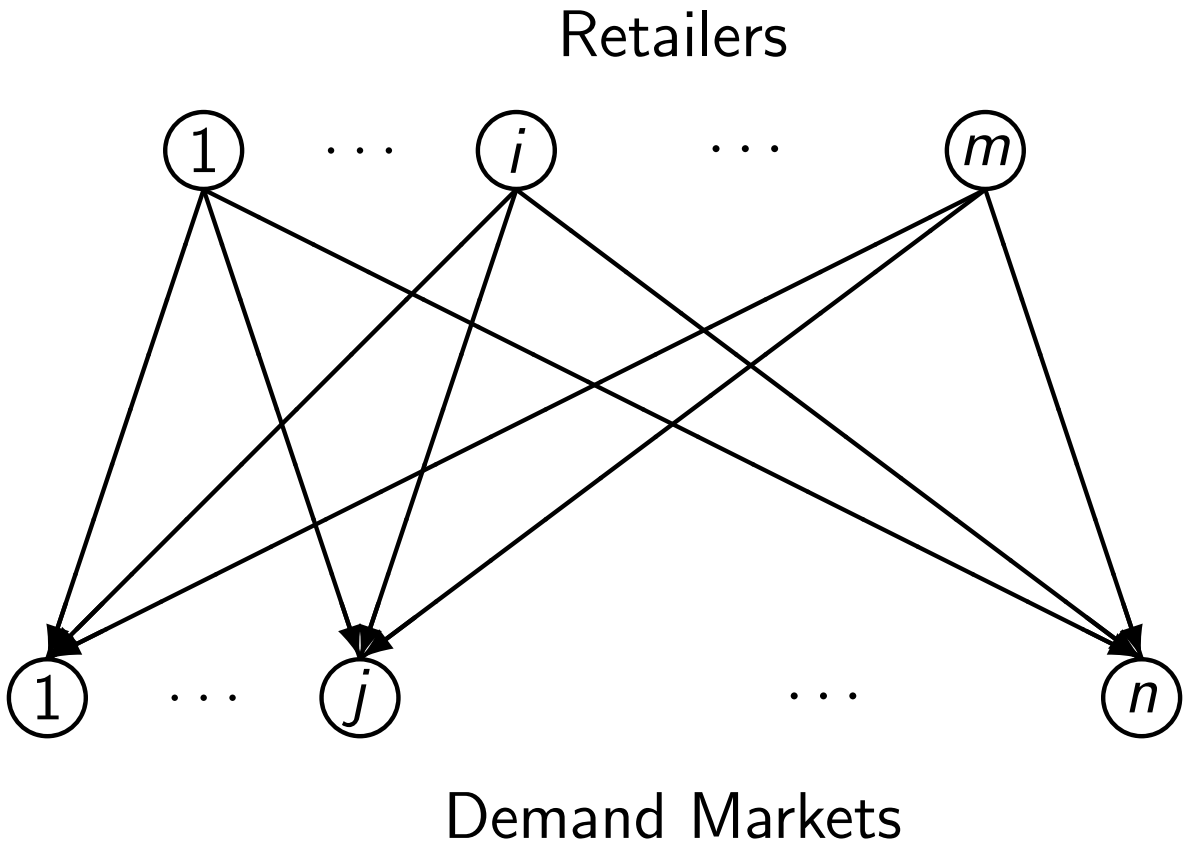


Figure: The Structure of the Supply Chain Network Game Theory Model

Some More of Our Recent Work

A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability, A. Nagurney, L.S. Nagurney, and S. Shukla (2015), in: *Computation, Cryptography, and Network Security*, N.J.Daras and M.Th. Rassias (Eds.), Springer, pp 381-398.

A Game Theory Model of Cybersecurity Investments with Information Asymmetry, A. Nagurney and L.S. Nagurney (2015), *Netnomics* 16(1-2), pp 127-148.

A Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints, A. Nagurney, P. Daniele, and S. Shukla (2016), in press in *Annals of Operations Research*.

Cybersecurity Investments with Nonlinear Budget Constraints: Analysis of the Marginal Expected Utilities, P. Daniele, A. Maugeri, and A. Nagurney (2016), in press in *Operations Research, Engineering, and Cyber Security*, Th.M. Rassias and N.J. Daras (Eds.), Springer International Publishing.

Summary and Conclusions

- In the final part of this lecture, we overviewed our work on **network vulnerability** from a cybersecurity perspective. Our "clients" were retailers and energy corporations, who have also encountered a **growing number of cyberattacks**. Additional results we have obtained for case studies in financial services.

Summary and Conclusions

• In the final part of this lecture, we overviewed our work on **network vulnerability** from a cybersecurity perspective. Our "clients" were retailers and energy corporations, who have also encountered a **growing number of cyberattacks**. Additional results we have obtained for case studies in financial services.

• The cybersecurity investment models that we prevented included Nash Equilibrium, Nash Bargaining, as well as System-Optimization models. **The results demonstrate the relevance of cooperation with the most practical cooperative model being that of Nash Bargaining**.

Summary and Conclusions

• In the final part of this lecture, we overviewed our work on **network vulnerability** from a cybersecurity perspective. Our "clients" were retailers and energy corporations, who have also encountered a **growing number of cyberattacks**. Additional results we have obtained for case studies in financial services.

• The cybersecurity investment models that we prevented included Nash Equilibrium, Nash Bargaining, as well as System-Optimization models. **The results demonstrate the relevance of cooperation with the most practical cooperative model being that of Nash Bargaining**.

• Our research integrates inputs from practitioners with the goal of providing prescriptive analytics for decision-making for cybersecurity investments.