Game Theoretic Modeling to Enforce Security Information Sharing among Firms

Deepak K. Tosh[†], Shamik Sengupta[†*], Sankar Mukhopadhyay[‡]
[†]Dept of Computer Science and Engineering
[‡]Dept of Economics, University of Nevada, Reno
Email: dtosh@unr.edu, ssengupta@unr.edu, sankarm@unr.edu

Charles A. Kamhoua, Kevin A. Kwiat
Air Force Research Laboratory
Cyber Assurance Branch, Rome, NY
Charles.Kamhoua.1@us.af.mil, Kevin.Kwiat@us.af.mil

***Abstract*—Robust CYBersecurity information EXchange (CYBEX) infrastructure is envisioned to protect the firms[1] from future cyber attacks via collaborative threat intelligence sharing, which might be difficult to achieve via sole effort. The executive order from the U.S. federal government clearly encourages the firms to share their cybersecurity breach and patch related information among other federal and private firms for strengthening their as well as nation's security infrastructure. In this paper, we present a game theoretic framework to investigate the economic benefits of cyber-threat information sharing and analyze the impacts and consequences of not participating in the game of information exchange. We model the information exchange framework as distributed non-cooperative game among the firms and investigate the implications of information sharing and security investments. The proposed incentive model ensures and self-enforces the firms to share their breach information truthfully for maximization of its gross utility. Theoretical analysis of the incentive framework has been conducted to find the conditions under which firms' net benefit for sharing security information and investment can be maximized. Numerical results verify that the proposed model promotes such sharing, which helps to relieve their total security technology investment too.**

***Index Terms*—Cyber-threat intelligence, Information exchange, Game theory, CYBEX**

I. Introduction

The information-centric world has been revolutionized via efficient utilization of cyberspace and provisioning IT services towards end-users convenience. From simple record keeping to military operations, highly secured business transactions are performed using networked systems where, proprietary/private information are exchanged among them to enable personalized services. Though on hand, these internetworked systems brought many technical solutions for business owners and end users, but on the other hand malicious cyber thieves always look for system loopholes to sneak in and exploit the organizations' intellectual properties for achieving financial advantage. Recent cyber attack victims include U.S. retail chains such as Target Corp, Neiman Marcus, Home Depot; financial corporations like JP Morgan and Chase; health insurance companies like Primera Blue, Anthem. which have faced cyber attacks and reportedly [1][2] millions of customers personal record including social security numbers have been stolen. The cyber attacks do have adverse effect on firms' productivity as well as on nation's integrity, therefore securing all assets from the cyber thieves is currently a prime focus of most organizations.

Isolated research on cybersecurity threats analysis and developing anti-threat strategies by individual firms may not be very effective to tackle cyber crimes [3][4] unless they have timely information on the particular vulnerabilities. It may not be a cost-effective approach to act independently, when a firm finds that it has been compromised by an attacker and tries to develop a countermeasure at the earliest by investing money and time in its security R&D. Cooperation to share this information with other organizations would have helped to quickly find an already developed countermeasures for the breach at reduced investment. Hence, voluntary exchange of cyber-threat intelligence such as type of vulnerability, IP addresses and domain names, URLs involved with attacks, intrusion signature patterns, malware analysis report, type of network traffic, origin information, adversary tactics, mitigation strategies etc, can be handy for firms to explore root causes and act in a timely manner. Considering the potential of such information sharing, U.S. congress house has recently passed a bill [4][5] promoting exchange of cybersecurity information.

Currently, firms hesitate to share their security information with other federal agencies and firms due to several following reasons: *(1) negative publicity might affect their market value and stock price, (2) sharing of security holes with competing firms can be risky if rivals violate trust [6] and take advantage of the breach reporting firm directly or indirectly with the help of third-party agents, (3) federal law violations might be revealed to federal agencies*. However, vulnerability information sharing among firms has more benefits in the long run, such as: *(1) prevention of future cyber attacks and revenue loss by finding and repairing the vulnerabilities proactively, (2) sharing breach information with a standardized central monitoring system governed by federal agencies can be a strong reason to assure their customers about the security measures undertaken, which will allay the customers' perceived security risk, (3) cost of investment in developing countermeasure to cyber attacks is higher compared to collaborative efforts on strengthening security.*

• Approved for Public Release; Distribution Unlimited: 88ABW-2014-1521
*This research is supported by the National Science Foundation (NSF) Award #1528167.

[1] The term "firm" refers to any organization, institution, industry, federal agency that can be target of cyber crimes.

To enable security information sharing, ITU-T took initiative to adopt a cybersecurity information exchange (CYBEX) [7] that imports more than twenty best standards developed by different agencies to tighten cybersecurity and infrastructure protection. To enable such sharing service, a promising set of protocols/specifications: STIX, TAXII, CybOX, etc. [8] have been designed for efficient threat analysis, structured language for threat information, secure sharing services. Security information sharing has been studied extensively in the past where a centralized social planner coordinates the information exchange process among the firms so that production efficiency is maximized. [9] studied a 2-firms game model by focusing on demand side effects on their utility to understand sharing benefits. [3][10] discusses the trade-off between breach information sharing and security investment in a two-firms game setup where major decisions are controlled by a social planner. To gauge a firm's attractiveness towards cyber attacks and determining how much security investment is required, a model is proposed in [11] by considering both serial and parallel data theft. Quantifying the cost associated with IT security breaches and impacts of breach information transfer on its market value is studied in [12]. Authors of [13] presented a two-stage Bayesian game between two firms utilizing a common platform.

Majority of the research works consider centralized framework, where the firms inherently cooperate with each other and their decisions are driven by the social planner. However, in a real world scenario, firms do compete with each other for more market share and revenue in a distributed and non-cooperative manner. Additionally, business conflict and lack of trust among each other might hinder them to share their cyber-threat intelligence. Hence, it is required to devise distributed sharing mechanisms where firms can make independent decisions regarding the amount of threat intelligence to share and security investment to make. *Moreover, it is necessary to model self-enforcement mechanisms for the firms to participate in the information sharing framework, which in turn maximizes their social welfare and security robustness.* In our past research [14][15], we have introduced external incentivization by CYBEX to self-enforce the firms toward participate and share their cyber-threat knowledge using an evolutionary and a non-cooperative game model respectively.

In this paper, we model the threat-intelligence information sharing as a distributed and non-cooperative game among N firms and propose an incentive framework to foster their information sharing behavior. Since such exchange process helps everyone to boost their security issues, which is modeled as incentive from the framework, it costs them too in terms of market value and reputation etc. This trade-off has been considered for formulating a robust utility model that is scalable to any number of firms, to reward them based on their information sharing and willingness to invest. Since the firms' net benefit is not only driven by their own security investment and sharing intentions, but also on other firms' decision parameters, individual benefit maximization requires every firm to play with their best-response strategy so that socially optimal equilibrium can be achieved. Therefore, we analyze this non-cooperative game to find the best response investments and information sharing amount from a firm's perspective, which will optimize its net reward. Moreover, we deduce the general condition under which such socially-optimal situation could be achieved. The reported simulation results describe the positive aspects of information sharing on cost of security investment as well as overall utility gain.

The rest of the paper is organized as follows. Section II describes the system model of information exchange game and proposed incentive model by defining each components. The optimization problem and the best response analysis are presented in section III to find the best response investment levels and self-enforcement conditions for motivate the firms to share. Numerical and simulation results are reported in section IV with explanation. Conclusions and future research directions are presented in last section.

II. System Model and Game Formulation

We consider a market scenario, where N firms are playing in this game aiming to strengthen their cybersecurity infrastructure via security investments and breach/patch related information sharing. Without loss of generality, we assume that each firm i invests $I_i \in [0,1]$ amount of its total annual investment budget towards security development and decides to share $l_i \in [0,1]$ amount of the total breach/patch related information with other firms at a decision point.

A. Security Information Exchange Game

The security information exchange game, $G = (N, S, U)$ is played in a distributed manner among the N firms, where i^{th} firm has two variable continuous strategy space $S_i = \{(I_i, l_i) : l_i \in [0,1], I_i \in [0,1]\}$. To compensate the cost of information loss due to successful cyber crime and defend future cyber attacks, the firms (1) consider monetary investment for further advancements in security, and (2) share the vulnerability information set with other firms or central information exchange for collaborative effort. The rational entities face the optimization problem to find the best response strategy of maximizing overall payoff where, cost of both security investment and information sharing of the firm is minimized. The strategy profile, $s = \{s_1, s_2, ...s_N\} \in \hat{S}$, constitutes set of individual strategies for networks $1, 2, ...N$ where, $\hat{S} = S_1 \times S_2 \times ... \times S_N$. By taking strategy S_i, the firm decides to exchange l_i amount of vulnerability information and invests I_i amount towards security technology.

The devised utility equation incentivizes the firms for better contribution to the information exchange framework and the firms are expected to figure out the corresponding equilibrium strategies that maximize their overall payoff. Using cost-benefit approach, the utility expression for the game G is formulated which considers sharing gain, cost of security investment, relative cost of security information exchange, and cost of processing the collected information. In practice, many other cost and benefit components like stock value, market reputation, customer satisfaction ability can be considered in incentivizing a firm to bolster security information sharing. But for the sake of tractable analysis of the proposed game theoretic model, we consider the four above discussed major components in this work, which are briefed in the following subsections.

B. Sharing and Investment Gain

In addition to the direct benefits from a firm's own investment, it also receives indirect gain from other firms' shared information on vulnerability patches and fixes. So the overall gain to a firm not only depends on own security investment, but also on the other firms' sharing intentions, and their investment levels. To model the indirect gain from other firms, we assumed a quadratic function to measure the benefits of shared information from every other firm. However, any increasing function instead of quadratic can also be applied to model the information sharing benefits. A logarithmic gain function G_i for firm i is considered to model the total utility gain from overall direct investment and indirect sharing benefits.

$$G_i(S_i, S_{-i}) = f(N) \log \left(I_i + \sum_{j \neq i}^{N} \beta_{ij}(I_j + \tau \sum_{k \neq j}^{N} l_k^2) \right) \quad (1)$$

The logarithmic gain function motivates the players by returning high reward at small steps towards information sharing and security investment. However, the reward saturates at high value of investment and information sharing, which explains that high investment does not necessarily increase the overall utility, rather reducing the investment level and increasing sharing level will return similar reward incurring less cost.

The scaling parameter τ scales the investment and total value of competing firms' shared information to equivalent dimension, and the parameter β_{ij} represents the conversion parameter that maps the usefulness of firm j's shared information based on firm i's security requirement. The value of β_{ij} becomes zero, when firm j does not share any security related information with firm i. $f(N)$ represents the gain scaling function of number of participants in the information exchange game, which helps to incentivize the players more when the number of participants in the game increases. Therefore, more firms will be attracted to share their security information, which will eventually enhance the individual gross utility.

C. Cost of Security Investment and information exchange

The process of combating current/future cyber attacks requires help from other competing firms as well as monetary investment towards firm's own security task force. The help-seeking firm is less likely to receive any vulnerability related information or preventive mechanisms from other experienced firms until it exchanges its own breach/patch related information with others. However, this security information exchange is associated with the risk of tarnished reputation along with its market value, and customer base. In this work, the information sharing enabled cyber defense approach of a firm involves three types of cost parameters: (1) direct monetary cost for own security investment $C_T(I_i)$, (2) cost of information sharing $C_S(l_i, l_{-i})$, which is relative to other firms' sharing intentions (l_{-i}), and (3) processing cost $C_P(l_{-i})$ of the received security information from other firms excluding i. The total cost to firm i can be expressed as:

$$C_i(I_i, l_i, l_{-i}) = \theta_1 C_T(I_i) + \theta_2 C_S(l_i, l_{-i}) + \theta_3 C_P(l_{-i}) \quad (2)$$

where, $0 \leq \theta_1, \theta_2, \theta_3 \leq 1$ are the scaling constants emphasizing the cost of investment and information sharing respectively.

Intuitively, the investment cost function, $C_T(I_i)$ must increase when firm i increases its security investment I_i, i.e. $\frac{\partial C_T}{\partial I_i} > 0$. The cost of information sharing $C_S(.)$ increases as firm i increases its information sharing level, i.e. $\frac{\partial C_S}{\partial l_i} \geq 0$. However, this information sharing cost is relieved, when every firm simultaneously exchanges its security information with each other, because the customers perceive this action as a positive step towards defending against cyber crimes. Hence the firm's market value, customer satisfaction, and reputation is likely to unaffected when everybody support security information exchange, i.e. $\frac{\partial C_S}{\partial l_j} \leq 0$, $\forall j \neq i$. The example cost function of information sharing given in Eqn. 3 satisfies the above-mentioned properties, which is a sum of relative sharing intentions times total shared information in the interaction, with respect to every other firm.

To retrieve the best out of the collected security information from different firms, it is required to filter out the relevant information and process them according to firm i's requirements. This requires an extra effort and cost to be invested for effective utilization of the collected information, thus the cost of information processing can be expressed in Eqn. 4.

$$C_S(l_i, l_{-i}) = \sum_{j \neq i}^{N} (l_i + l_j)(l_i - l_j) = \sum_{j \neq i}^{N} (l_i^2 - l_j^2) \quad (3)$$

$$C_P(l_{-i}) = \sum_{j \neq i}^{N} \gamma_{ij} l_j \quad (4)$$

where, $\gamma_{ij} \in [0, 1]$ represents the firm i's processing overhead to extract out and process the useful information from the firm j's ($j \neq i$) shared information set.

III. Optimization Problem

The cost-benefit analysis of information exchange game requires to find the best response values of decision variables such as investment and sharing level. The firms suitably change the values of their decision parameters to optimize its net utility, however this cannot be achieved without co-operation of other firms. It is expected that the proposed incentive mechanism will self-enforce security information sharing among the participating firms which in turn will reduce the investment costs of individual participants. Also, when the number of firms involved in the game increases and they truthfully exchange their vulnerability information, the overall gain is improved at minimal cost for information sharing. The unconstrained optimization problem of choosing best response investment and sharing level decision can be found by maximizing the objective function given in Eqn. 5, which is formulated by combining the gain and cost components from Eqn. 1 and Eqn. 2 respectively.

$$
\begin{aligned}
&\underset{l_i, I_i}{\text{Maximize}}\ U_i(S_i, S_{-i}) \\
&= f(N)\log\left(I_i + \sum_{j\neq i}\beta_{ij}(I_j + \tau\sum_{k\neq j}^{N} l_k^2)\right) \\
&-\theta_1 C_T(I_i) - \theta_2((N-1)l_i^2 - \sum_{j\neq i}^{N} l_j^2) - \theta_3\sum_{j\neq i}^{N}\gamma_{ij}l_j \qquad (5)
\end{aligned}
$$

A. Best Response Analysis

The objective function presented in Eqn. 5 needs to be maximized with respect to a firm's security investment (I_i^*) as well as sharing intention level (l_i^*), assuming other players keep their investment and sharing intentions as their best responses. Hence, for finding I_i^* , $\frac{\partial U_i(.)}{\partial I_i} = 0$ and $\frac{\partial^2 U_i(.)}{\partial I_i^2}\ |_{I_i = I^*} < 0$ must be satisfied. Assuming $Z = I_i + \sum_{j\neq i}\beta_{ij}(I_j + \tau\sum_{k\neq j}^{N} l_k^2)$, the following needs to be computed,

$$\frac{\partial U_i(.)}{\partial I_i} = \frac{f(N)}{Z} - \theta_1 C_T'(I_i) = 0 \qquad (6)$$

Assuming $I_i = I^*$ is the best response investment level, then the following open form equation must be satisfied.

$$I_i^* = \frac{f(N)}{\theta_1 C_T'(I_i^*)} - \sum_{j\neq i}\beta_{ij}(I_j + \tau l_i^2) \qquad (7)$$

$$\frac{\partial^2 U_i(.)}{\partial I_i^2} = -\frac{f(N)}{Z^2} - \theta_1 C_T''(I_i) \qquad (8)$$

From Eqn. 8, it is clear that $\frac{\partial^2 U_i(.)}{\partial I_i^2} < 0$, provided $C_T''(I_i) > 0$ and for positive value of investment, $\frac{f(N)}{\theta_1 C_T'(I_i)} > (\sum_{j\neq i}\beta_{ij}(I_j + \tau\sum_{k\neq j}^{N} l_k^2))$ must be satisfied.

To promote security information sharing, the firms should be rewarded more with increase in their sharing intentions. Thus, the best response value of l_i should be the maximum value that it can take, and the gross utility of firm i presented in Eqn. 5, must be an increasing function w.r.t l_i, when the investments and sharing intentions of other firms are constant. The condition presented in theorem 3.2 must be satisfied to self-enforce the firms to share their security information.

Definition 3.1: A continuous function $f(x)$ is said to be increasing in the interval $[a, b]$, if its first order differential $f'(x)$ is positive ($f'(x) > 0$) between the given interval.

Theorem 3.2: The gross utility function $U_i(.)$ increases with respect to firm i's sharing intention in the range $\{(l_i^1, l_i^2) : l_i^1 < l_i^2\}$ provided the following condition is satisfied.

$$\frac{Z(l_i^1)Z(l_i^2)}{I_i + \sum_{j\neq i}\beta_{ij}(I_j - \tau l_i^1 l_i^2)} < \frac{2f(N)\tau\sum_{j\neq i}\beta_{ij}}{2\theta_2(N-1)}$$

Proof: For proving the increasing nature in range (l_i^1, l_i^2), where $l_i^1 < l_i^2$ it is required to show that,

$$
\begin{aligned}
&\frac{\partial U_i(.)}{\partial l_i}\ |_{l_i^2} - \frac{\partial U_i(.)}{\partial l_i}\ |_{l_i^1} > 0 \\
&\frac{\phi_1 l_i^2}{\phi_2 + \phi_3(l_i^2)^2} - \frac{\phi_1 l_i^1}{\phi_2 + \phi_3(l_i^1)^2} > 2\theta_2(N-1)(l_i^2 - l_i^1) \\
&\frac{\phi_1(\phi_2 - \phi_3 l_i^1 l_i^2)}{(\phi_2 + \phi_3(l_i^1)^2)(\phi_2 + \phi_3(l_i^2)^2)}) > 2\theta_2(N-1) \\
&\frac{Z(l_i^1)Z(l_i^2)}{I_i + \tau\sum_{j\neq i} l_j^2 + \sum_{j\neq i}\beta_{ij}(I_j - \tau l_i^1 l_i^2)} < \frac{\phi_1}{2\theta_2(N-1)} \qquad (9)
\end{aligned}
$$

where, $\phi_1 = 2f(N)\tau\sum_{j\neq i}\beta_{ij}, \phi_2 = I_i + \sum_{j\neq i}\beta_{ij}(I_j + \tau\sum_{k\neq j,i}^{N} l_k^2), \phi_3 = \sum_{j\neq i}\beta_{ij}\tau$.

Remarks: The above proved condition ensures that the firms will have higher benefits if they share more breach related information among each other. Hence, this condition helps to self-enforce the firms to participate in the sharing framework and share as much information as they can. Thus, it will (in)directly return a high utility reward to the firms and they can reciprocate the same behavior of exchanging security information to eventually reach an equilibrium state.

IV. Simulation results and analysis

We studied the nature of the information sharing framework via numerical analysis and simulations to show that the firms can be benefited more via breach/patch related information exchange. We present the results from static single stage analysis of the incentive model for two and more than two participating firms ($N = 2, 4,$ and 20), where the overall utility rewards are reported by varying their information sharing intentions as well as investment levels. We assume that 80% of the collected shared information are useful for each firm, so β_{ij} is set to be 0.8. As the investment cost function $C_T(I_i)$ presents the monetary cost of a firm towards security investment, we assume a quadratic function, where low investments return low cost but high investments increase the cost C_T rapidly. This factor can motivate the firms to participate in information exchange instead of making large security investments while defending cyber crimes. To promote information sharing, we consider a quadratic gain scaling function $f(N) = aN^2 + bN + c : a, b, c \in \mathbb{R}$, which triggers high reward when a large number of firms join the information exchange framework. However, the nature of gain scaling function is not limited to only quadratic, rather any strictly increasing function of N can be a candidate $f(N)$.

In Figure 1, and 2, we studied the nature of overall utility variation with respect to firm i's security investment levels by varying its information sharing intentions in a two-firms and 20-firms market scenario respectively. In this scenario, it is assumed that all other firms keep their investment level to 0.5 and fully share their security breach/patch information, i.e. $l_j = 1 \forall j \neq i$. When firm i' increases its information sharing intention as well as it is willing to invest, we observe that there exists a best response investment level beyond which the investment cost dominates over the total gain. The best

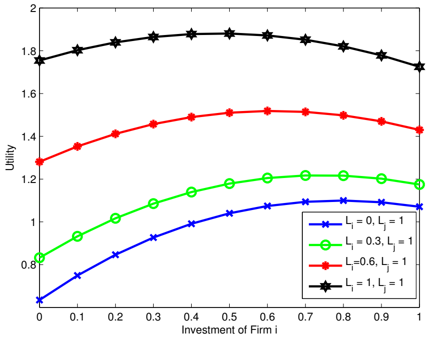

Fig. 1: Optimal Investment on own sharing level variation ($N = 2$)

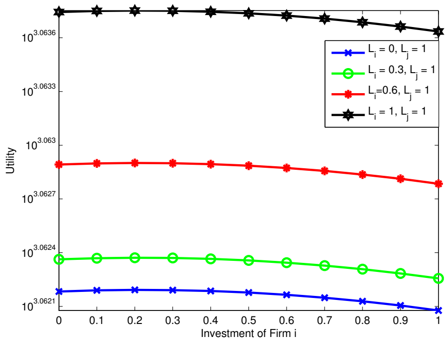

Fig. 2: Optimal Investment on own sharing level variation ($N = 20$)

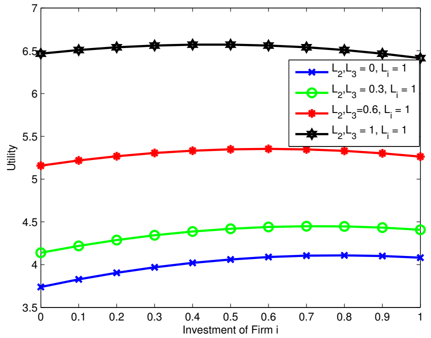

Fig. 3: Effect of others' sharing level on Firm i's investment

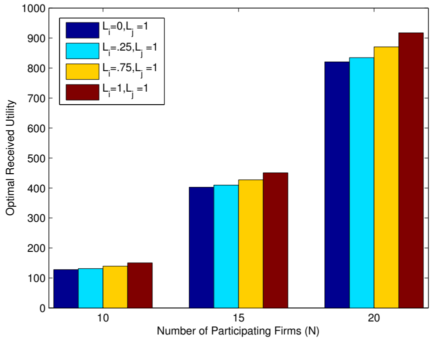

Fig. 4: Utility Vs. Number of participating firms

response value of investment apparently reduces as firm i increases its information sharing limit irrespective of other firms' actions. On another note, it can be stated that when the firm j truthfully shares its information, firm i cannot maximize its utility reward until it increases its information sharing level. Hence, the firms are required to self-enforce themselves towards information sharing to receive high payoff. To study the scalability of the framework, the same characteristics is experimented when $N = 20$ firms participate and it is observed that the gross utility to the considered firm is increased whereas the best response investment level representing the maximum utility is reduced compared to scenario of less number of participating firms. Therefore, the framework attracts more firms to participate in information sharing activity to receive maximum payoff.

In Fig. 3, we present the effect of other firms' sharing levels on firm i's utility reward with respect to i's own security investment level, when the number of participating firms (N) is 4. Assuming two firms simultaneously change their information sharing levels from 0 to 1 with an increment of 0.25, it is observed that when other firms do not share anything, the reward to the firm i is minimal. But we have seen from Fig. 1 that the firms who decrease their sharing limits, suffer with low utility reward. Hence, no single firm cannot gain more by reducing its information sharing limit, which self-enforces the rational firms to share more information to maximize their individual utility as well as system utility. Assuming 50% of the total participating firms fix their investment and sharing level to 0.5 and 1 respectively, Fig.4 presents the behavior of total utility value to a firm when number of participating firms vary from 10 to 20. It is observed that the utility value increases with growing rate of participants in the exchange framework when they share maximally irrespective of other firm's sharing intentions. Therefore, the framework can adapt high number of participants and self-enforce the firms to exchange more by rewarding high payoffs.

Figure 5 presents the utility reward to firm i, when it unanimously changes its level of information exchange. We experimented to find how firm i's security investment affects its overall received utility by varying its sharing level. It is clear from the plot that sharing more information can drive them to achieve high reward. Hence the profit-seeking firm i should always choose to share maximally with $l_i = 1$. Another point can be noted that minimum investment rewards minimum utility, however, a firm can improve its received reward gain by increasing its information sharing activity. Hence, the firms need to both invest a non-zero amount, and voluntarily share their vulnerability related information with other firms to receive maximum utility.

Figure 6 and 7 show the utility variation when some firms decrease their security investments and try to free-ride on the other firms' shared information for cases of $N = 4$ and $N = 20$ respectively. It can be observed that when a firm $j(\neq i)$ reduces its security investment level then the overall utility of firm i is negatively affected. As per the simulation conditions, majority of the participating firms are sharing their security information, hence firm i can compensate the utility loss by increasing its information sharing level. From the previous results, we have seen that no firm can improve its payoff by making low security investment, hence the firms may not choose to free-ride by making very minimal investment or minimal information sharing due to the possibility

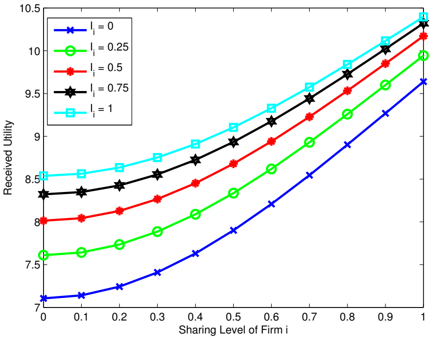

Fig. 5: Effect of Firm i's sharing level on received utility w.r.t. own investment level variation $(N = 4)$

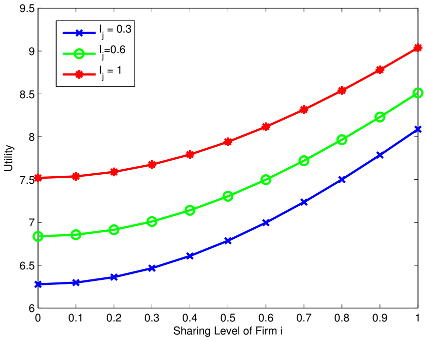

Fig. 6: Effect of Firm i's sharing level on received utility w.r.t. other firms' investment level variation $(N = 4)$

of getting penalized with low utility reward. In the reported plot, we have showed that the reward value decreases when only one of the competing firms reduces its investment level, keeping its sharing intention high. It can be easily inferred that the reward value will be even lesser, when many firms will make minimal investment and information sharing. Figure 7 is reported to show that the behavior of framework remains unchanged even when the number of participating firms rises. Hence the framework can effectively self-enforce every firm to maximally share its breach/patch related information.

V. Conclusions and Future Research Directions

Cyber attacks and cyber crimes can be eradicated easily via collaborative information sharing among firms instead of working and investing individually. The collaborative effort is facilitated via sharing of breach related information with other competing firms, however a proper incentive framework is required which can self-enforce the firms to voluntarily share their security information and can make suitable security investments to develop stronger counter-measures. In this work, we modeled a simultaneous information exchange game and proposed an incentive framework by considering positive and negative aspects of breach/patch information sharing and security technology investment. The incentive model is verified via numerical analysis under scenarios of varying investment levels, and sharing intentions of the considered firms as well as from competing firms' perspective. It is found that firms are incentivized more when they share more information among each other and firms' security investments additionally help to maximize the received utility. The sharing nature also helps the firms in reducing their cost of investment in the long run too. In the future, we plan to design a multi-stage repeated game approach for the firms to act independently in a distributed manner for maximizing the overall utility via learning from the past accumulated history information. We also aim to design an insurance-based mechanism to incentivize and penalize firms on their sharing and non-sharing behavior respectively.

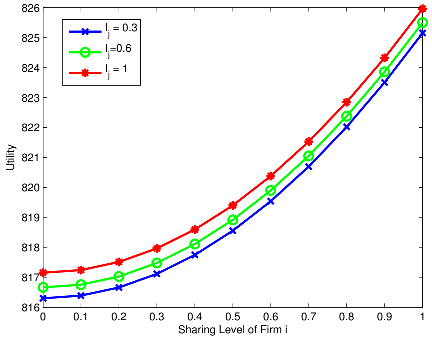

Fig. 7: Effect of Firm i's sharing level on received utility w.r.t. other firms' investment level variation $(N = 20)$

References

[1] http://www.informationweek.com/security/attacks-and-breaches/neiman-marcus-target-data-breaches-8-facts/d/d-id/1113415.

[2] http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html.

[3] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Sharing information on computer systems security: An economic analysis," *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461–485, 2003.

[4] E. A. Fischer, E. C. Liu, J. W. Rollins, and C. A. Theohary, "The 2013 cybersecurity executive order: Overview and considerations for congress," 2013.

[5] "Cybersecurity information sharing act of 2015, https://www.congress.gov/114/bills/s754/bills-114s754pcs.pdf."

[6] S. Bowles, *Microeconomics: behavior, institutions, and evolution*. Princeton University Press, 2009.

[7] A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin, T. Takahashi, C. Schultz, G. Reid, G. Schudel, M. Hird, and S. Adegbite, "Cybex: The cybersecurity information exchange framework (x.1500)," *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 5, pp. 59–64, Oct. 2010. [Online]. Available: http://doi.acm.org/10.1145/1880153.1880163

[8] P. Kampanakis, "Security automation and threat information-sharing options," *Security & Privacy, IEEE*, vol. 12, no. 5, pp. 42–51, 2014.

[9] E. Gal-Or and A. Ghose, "The economic consequences of sharing security information." *Economics of information security*, vol. 12, pp. 95–105, 2004.

[10] D. Liu, Y. Ji, and V. Mookerjee, "Knowledge sharing and investment decisions in information security," *Decision Support Systems*, vol. 52, no. 1, pp. 95 – 107, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167923611001151

[11] S. E. Schechter and M. D. Smith, "How much security is enough to stop a thief?" in *Financial Cryptography*. Springer, 2003, pp. 122–137.

[12] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," *International Journal of Electronic Commerce*, vol. 9, no. 1, pp. 70–104, 2004.

[13] M. Khouzani, V. Pham, and C. Cid, "Strategic discovery and sharing of vulnerabilities in competitive environments," in *Decision and Game Theory for Security*. Springer, 2014, pp. 59–78.

[14] D. K. Tosh, S. Sengupta, C. Kamhoua, K. A. Kwiat, and A. Martin, "An evolutionary game-theoretic framework for cyber-threat information sharing," in *Proceedings of the IEEE International Conference on Communications (ICC)*, 2015.

[15] D. K. Tosh, M. Molloy, S. Sengupta, C. Kamhoua, and K. A. Kwiat, "Cyber-investment and cyber-information exchange decision modeling," in *Proceedings of the IEEE Cyberspace Safety and Security (CSS)*, 2015.