Cyber-Investment and Cyber-Information Exchange Decision Modeling

D.K. Tosh, M. Molloy, S. Sengupta
Dept of Computer Science and Engineering
University of Nevada, Reno
dtosh@unr.edu, mmolloy@nevada.unr.edu, ssengupta@unr.edu

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

***Abstract*—Inefficiency of addressing cybersecurity problems can be settled by the corporations if they work in a collaborative manner, exchanging security information with each other. However, without any incentive and also due to the possibility of information exploitation, the firms may not be willing to share their breach/vulnerability information with the external agencies. Hence it is crucial to understand how the firms can be encouraged, so that they become self-enforced towards sharing their threat intelligence, which will not only increase their own payoff but also their peers' too, creating a win-win situation. In this research, we study the incentives and costs behind such crucial information sharing and security investments made by the firms. Specifically, a non-cooperative game between N-firms is formulated to analyze the participating firms' decisions about the information sharing and security investments. We analyze the probability of successful cyber attack using the famous dose-response immunity model. We also design an incentive model for CYBEX, which can incentivize/punish the firms based on their sharing/free-riding nature in the framework. Using negative definite Hessian condition, we find the conditions under which the social optimal values of the coupled constraint tuple (security investment and sharing quantity) can be found, which will maximize the firms' net payoff. The numerical results also verify the existence of socially-optimal solutions for the cyber-threat information exchange problem.**

***Index Terms*—Cybersecurity information sharing, CYBEX, Game theory, Dose-response immunity model**

I. Introduction

Rising rate of cyber criminal activities in health, energy, financial, retail, technology etc. sectors have posed a high-alert among the corporations [1][2][3][4] for protecting their proprietary assets. Therefore, information security has become a hard constraint for them to expand their businesses around the globe, which reveals the importance of investment on cybersecurity. The intensity of cyber attacks may not be completely abated with sole investment only, when the firms do not possess the relevant actionable cyber-threat intelligence to efficiently act at the decision event [5][6]. However, with the cooperation from both federal as well as private companies via exchanging their cyber-threat intelligence, the corporations can access the timely information and act wisely to inhibit such malicious activities. Information about attackers' tools/methodologies can relieve the risk of exploitation, provided the firms share their threat intelligence among each other. Cyber-threat intelligence mainly refer to their threat indicators such as malicious reconnaissance, security vulnerabilities or any valuable attributes of the threat and the corresponding defensive measures. For instance, the threat information about an attack may contain attributes [7] 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., so that firms can discover the root causes of the attack instances. To thwart cyber-criminal acts by the malevolent cyberthieves, U.S. government promotes threat-information sharing among the companies as well as the federal agencies [8][9]. A promising set of protocols/specifications: STIX, TAXII, CybOX, etc. [10] have been designed for various information sharing services such as efficient threat analysis, structured language for threat information, secure sharing services etc.

Even though threat knowledge sharing of firms is a positive initiative to successfully defend the cyber attacks, it can have certain implications such as: (1) sharing of security information with competing firms might give them a choice to free-ride and take advantage of the shared information without reciprocating the sharing behavior; (2) exchanging proprietary information can be risky if rivals violate trust and take advantage of the breach reporting firm directly or indirectly with the help of third-party agents; (3) negative publicity might affect their market value and stock price. Thus appropriate incentive mechanisms for Cybersecurity Information Exchange (CYBEX) [11] are necessary to motivate the corporations towards threat intelligence sharing [12]. A Firm's selfish behavior in achieving higher gain by free-riding on others' threat knowledge might propagate to every other firm, and eventually every rational firm tries to free-ride, which in turn does not benefit anyone. Thus it is of utmost importance to have a self-enforcement mechanism for the firms to motivate them for exchanging their vulnerability discoveries truthfully. Additionally, when the firms realize the benefits of information sharing, they also need to decide how much investment to make and how much amount of threat intelligence to share in such non-cooperative setting.

Cybersecurity information sharing models have been investigated in the past by developing centralized microeconomics models [5][13][6], that focus mostly on improving the

**Approved for Public Release; Distribution Unlimited: 88ABW-2015-0337, Dated 28 Jan 2015.

production efficiency. Based on nature of information assets, the researches in [14][15] studied a 2-firms scenario on their investment and sharing decisions. Majority of these centralized frameworks also inherently assume the firms to be always cooperative with each other, while in a real world scenario, firms compete with each other for more revenue, market share, and shareholders in a distributed and non-cooperative fashion and they may not be willing to cooperate with each other due to business conflicts and lack of trust [16]. In the recent time, the research has presented increasing amount of evidence documenting systematic and predictable deviations and expansion from the classical notion of cooperation toward a more methodical preferential notion of rationality for adaptive and intelligent societies [17][18]. Departing from such centralized paradigm, firms prefer to interact in a distributed and non-cooperative fashion where they can independently decide how much investment to make and information to share instead of relying on an external agent's decision. To self-enforce firms towards sharing, an evolutionary game is modeled in our past work [19] where CYBEX intelligently varies the participation cost so that firms are triggered towards participation. If the firms choose to share, the underlying challenge is to balance the amount of shared information and security investment so that the success probability of future cyber attack will be reduced. This underscores the following critical questions: (1) how much a firm should exchange out of its total discovered information? (2) what amount of investment will be sufficient in the presence of information exchange? (3) how CYBEX can motivate the firms by providing incentives (in a dynamic manner) yet make the sharing system self-sustained so that sharing is done directly rather than through external means?

Assuming CYBEX [11] provides a secure medium to share the threat information, we consider that it collects the shared information from each participating firm and forwards the aggregated information back to all participants. It also helps to motivate and self-enforce the firms towards sharing activity by using appropriate incentivization mechanism. Considering the conflicts of information exchange process, we propose a simultaneous non-cooperative game-theoretic solution to resolve the conflict of deciding how much security investment to be made and breach information to be shared with CYBEX such that their expected utility is maximized. The effectiveness of information sharing also affects the firms' defending ability from future cyber attacks, which is formalized using a dose-response immunity model. Eventually, we derive the conditions at which the firms can achieve socially-optimal equilibrium using Hessian negative definite condition. The simulation results also verify the existence of such equilibrium for the distributed non-cooperative information sharing game.

The rest of the paper is organized as follows. System model and the CYBEX self-coexistence game is formulated in Section II. Section III, analyzes the game to find conditions under which Nash equilibrium (NE) and the social optimality can be achieved. The insights for CYBEX to self-motivate firms to share more, is also detailed in this section. Section IV and V presents the numerical results and conclusions respectively.

II. System Model

Our model considers a simultaneous game between the participating companies where the breach information is exchanged through CYBEX. Thus, there are no direct interactions between the firms and for privacy issues, their identities are ensured to be hidden by CYBEX while exchanging the firms' findings. The corporations' strategies are twofold: investment, and vulnerability information exchange, where the technology investment helps them to conduct more research on the possible security breaches and the exchange strategy helps to reciprocate the sharing nature of others. The framework requires all participants to exchange their findings with CYBEX so that everyone can get the most benefits in terms of information on vulnerabilities, loopholes, bugs, fixes, corrupted programs etc. It is assumed that the firms have a maximum budget of $\mathcal{B}$ to invest for security, and total $\mathcal{L}$ amount of information to share. A firm's security investment is assumed to benefit only itself, however the received information helps both at the same time. Hence there is a possibility for some firms to free-ride on others information set, which must be prohibited to have a strategy-proof framework. CYBEX takes part in rewarding/punishing the firms based on their sharing attitude by via an incentive model.

A. Game Formulation

Consider a set of N corporations, denoted by $\mathcal{N} = \{1, 2, ..., N\}$, are participating in CYBEX information sharing framework. Assume that the firm $i \in \mathcal{N}$ has a total budget of $\mathcal{B}_i$ to invest on security and $\mathcal{L}_i \in \mathbb{N}$ amount of information related to a particular threat to share with CYBEX, hence forming the following strategy set for player i with sample space in $\mathcal{B}_i \times \mathcal{L}_i$.

$$S_i = \{(I_i, l_i) \in (\mathcal{B}_i \times \mathcal{L}_i) : 0 \leq I_i \leq \mathcal{B}_i \text{ and } 0 \leq l_i \leq \mathcal{L}_i\}$$

CYBEX collects the information set $L = \{l_1, l_2, ...l_N\}$ from N participants and forwards the aggregated information set (L_{-i}) to every firm $i \in \mathcal{N}$, which helps in improving the robustness of firm i, characterized by $\mathcal{F}(L_{-i})$. After receiving the aggregated information set from CYBEX, the firms evaluate the effectiveness of the played strategies through a payoff function U, described later.

In the above described game $G(\mathcal{N}, S, U)$, we consider the generic abstraction of "always rational and profit-seeking" CYBEX as well as firms. The conflict of the corporations in the game can be described as follows: the firms always look for securing their systems with minimum investment and sharing few/no breach information with CYBEX. However, low investment may not help in discovering/fixing the security issues, thus information sharing activity with CYBEX also goes down. This cost-saving instance might not benefit the firms at all, rather worsen the security issues. On the other hand, if they make very high investment and fully share, then the firms might not afford such a high cost in terms of monetary value and market value. Therefore, the corporations must choose their investments and amount of information to share very carefully so that their net benefit will be maximized.

From the CYBEX point of view, it aims to maximize the number of participants, because CYBEX receives a small percentage as participation fee from each participants too. Therefore, CYBEX's goal is to motivate as many participants to join in the framework and truthfully share their information, which will self-enforce other corporations to behave in similar way. In the next subsection, we model the firm's payoff function using a cost-benefit approach.

B. Utility Formulation

Table I lists the symbols and their meanings used throughout the paper. Now we model the firms' payoff, using several components described in the following.

TABLE I: Symbol Table

Symbol	Description
N	Total number of firms
$\mathcal{B}_i$	Total budget for firm i
$\mathcal{L}_i$	Total amount of information
I_i	Investment parameter
l_i	Sharing parameter
V_i	Asset value of firm i
α_i	Reward based on i's sharing effectiveness
$\zeta(l_i)$	Reputation loss function
β	Regression parameter for DRI model
p_i	Probability of encountering cyber attack
c_p	Cost of participation in CYBEX

1) Sharing and Investment Gain: If firm i decides to make a positive investment and share its threat discoveries with CYBEX, then it can receive two kinds of benefits: (1) direct gain from self-investment ($f_I(I_i)$) (2) robustness benefits from information sharing ($\mathcal{F}(L_{-i})$). The former gain, out of investment $I_i \leq \mathcal{B}_i$, can be defined as discovering various threat attributes, system loopholes, developing patches/fixes etc. The other firms' shared information contributes as indirect gain in terms of firm i's security robustness, which is represented by $\mathcal{F}(L_{-i})$. $\mathcal{F}$ is a function of total information shared in the system except the considered firm's contribution and it is assumed that the robustness value increases as the system's information sharing activity rises. The other factor, so called external incentive from CYBEX (α_i), also has an important role in the gain component. This external benefit aims to self-motivate the firms initially towards sharing more, but as the firms are self-enforced this incentive fades away gradually. The net benefit out of α_i is scaled up with respect to the amount of firm i's shared information (l_i) to provide the incentive in proportion to its information sharing activity. Assuming $\psi(l_i)$ is the function to reward a firm externally based on its nature of sharing, the generic gain function can be expressed as:

$$G(S_i, S_{-i}) = (\alpha_i \psi(l_i) + \mathcal{F}(L_{-i})) f_I(I_i) \tag{1}$$

The typical characteristics of investment gain function ($f_I(I_i)$) can be as follows: the firms can benefit at a higher rate until certain investment, however making an investment beyond this threshold limit does not reward much. Thus it can be modeled as a variant of logarithmic function [20] similar to $\log(1 + I_i)$. For rationality constraint, $\log(1 + I_i) > 0$, otherwise the firms would never invest. This gain saturates after a certain threshold and does not necessarily reward at a high rate. As described previously, the gain from information sharing constitutes, robustness advantage from other information, and external incentive (α_i) given by CYBEX based on its own sharing effectiveness, which is scaled according to a linear function $\psi(l_i)$, the joint gain out of both can be presented as:

$$G(S_i, S_{-i}) = a_0(\alpha_i l_i + \mathcal{F}(L_{-i})) \log(1 + I_i) \tag{2}$$

where, $a_0 > 0$ is a simple scaling parameter that maps user satisfaction/benefit to a dimension of the price/monitory value. The external incentive parameter (α_i) is crucial from the CYBEX's perspective, because it is modeled to motivate the individuals towards sharing their threat intelligence when the system of participants have not tasted the worth of sharing. However, when everyone is actively participating and sharing, then the incentive should fade away to let the sharing system self-sustained. In case of free-riding, the firm must be punished and no incentive will be given, so that the non-cooperation will be avoided. Therefore, the model for α_i for firm i can be a function of its own sharing (l_i) and the total information received from other firms except i. The following mathematical formula best capture the characteristics of (α_i) as described.

$$\alpha_i = \frac{\Gamma + l_i - \mathcal{F}(L_{-i})}{\mathcal{F}(L_{-i})} \tag{3}$$

where, $\Gamma = \sum_{i \in \mathcal{N}} \mathcal{L}_i$ is the maximum possible information exchanged in the sharing system by all the participating firms. $\mathcal{L}_i$ is the maximum amount of information that firm i can share with other firms. $\mathcal{F}(L_{-i}) = \sum_{j \neq i} l_j$. $\mathcal{F}(L_{-i})$ represents the aggregate information received by firm i and is assumed to be an increasing function of total information shared in the CYBEX framework. The detailed discussion of α_i is described later in Section III(B).

2) Cost Components Modeling: The information sharing activity costs a firm in several ways: (1) loss due to open access to protected assets, (2) reputation loss, (3) total investment, (4) participation cost, etc. Assuming the firm i has proprietary asset of value V_i, the firm's expected loss can be $p_i V_i$, where p_i is the probability of occurrence of an attack event at that particular decision period. We model this probability as a function of a firm's information sharing activity and the received information from CYBEX using dose-response immunity model, which is detailed later. The value of reputation loss for sharing l_i amount of information is presented as $\zeta(l_i)$. The reputation loss function is assumed to be an increasing function, which signifies that the reputation loss of a firm varies in proportional to its sharing activity. We assume the CYBEX participation cost to be $c_p > 0$, thereby formulating the total cost component due to information sharing as $C_s = p_i V_i + \zeta(l_i) + I_i + c_p$. Now, combining the components together, the net payoff of firm i playing with strategy S_i can be expressed as:

$$U(S_i, S_{-i}) = a_0(\alpha_i l_i + \mathcal{F}(L_{-i})) \log(1 + I_i) - C_s \tag{4}$$

C. Modeling p_i

The two major factors that influence probability of cyber attack on a firm are (1) degree of help from CYBEX ($\mathcal{F}(L_{-i})$),

(2) amount of information it exchanges with CYBEX (l_i). p_i is nothing but a risk evaluation parameter and the past researches in the field of medical sciences [21][22] have successfully used a method called dose-response model to quantify the hazard/risk posed by an inoculated dose of organisms. This model has also been applied in wireless networks [23] to detect covert communication by attackers. In the context of cybersecurity information sharing, [24] mentions that dose-response function can be used as a tool for representing uncertain events and cyber attack is one of them. Even though modeling probability of cyber attack based on a firm's sharing nature is always hard, the dose-response immunity (DRI) model can best capture the characteristics of cyber attack event according to our requirements. To appropriately model attack probability p_i, it must satisfy the following properties:

1) If a firm does not exchange any information, then its probability of getting attacked completely depends on the amount of information it receives for CYBEX and the security investment.
2) If every firm shares their information truthfully, then the total amount of information collected at CYBEX will be maximized and it could provide maximal benefit to each firm. As information sharing activity is maximal, the probability of cyber attack is expected to be diminished.
3) If CYBEX does not provide any help to the firms, due to the fact of no firm is interested to share, the probability of cyber attack completely depends on the security investment of the firms (as $l_i = 0$).

In the following, we mathematically interpret the generic DRI model and propose an equivalent form for p_i in brief.

Let the ability of a drug to recover from a disease be X_1 and X_2 refers the immunity power of the patient in response to the drug. Assume an event $Y \in \{0, 1\}$ denotes the survival of patient, where value 0 refers to fully survived and 1 refers to death of the patient. If $p = \Pr\{Y = 1\} = 1 - \Pr\{Y = 0\}$, then according to dose-response-immunity model,

$$\text{logit}(p) = \ln\left(\frac{p}{1-p}\right) = \beta^T \mathbf{X} \tag{5}$$

where, $\mathbf{X} = [X_1, X_2]^T$ and $\beta = [\beta_1, -\beta_2]^T$represents the regression vector. The negative sign is to represent the inverse nature of dose and immunity.

In our model, the amount of information exchanged (l_i) is analogous to dose of the drug and the received information from CYBEX is assumed to act as immune for the firm from cyber attacks. The event $Y = 1$ refers to a failure to defend a cyber attack and $Y = 0$ refers to successfully defend the cyber attack in our model. We assume that $\mathbf{X} = [\ln(1+l_i), \ln(\mathcal{F}(L_{-i}))]^T$. We consider $X_1 = \ln(1+l_i)$ because the probability of cyber attack may not be zero if a firm does not share anything.

Using dose-response-immunity model given in Eqn. (5), the probability of a cyber attack can be expressed as:

$$p_i = \frac{(1+l_i)^{\beta_1}}{(1+l_i)^{\beta_1} + (\mathcal{F}(L_{-i}))^{\beta_2}} \tag{6}$$

β_1 represents the effectiveness of firm i's shared information, and β_2 refers to the effectiveness of others' exchanged information in strengthening firm i's security.

D. Modeling Reputation Cost ($\zeta(l_i)$)

The reputation cost ($\zeta(l_i)$) is assumed to be an increasing function in terms of total number of threat intelligence shared with CYBEX, i.e. $\zeta'(l_i) > 0$. This emphasizes that the loss in firms' market value due to information exposure increases with increasing amount of shared information. However, we can also model this function as a convex function where, the firms regain their reputation after a certain limit due to the positive influence of cyber-threat exchange.

E. Optimization Problem

With the strategies and payoff model defined, the optimization problem for the firms in this game is to decide the optimal amount of information to share with CYBEX and the amount of security investment to make, so that the overall payoff will be maximized. As the payoff function of a firm is guided by its own actions as well as the sharing action of other players too. Hence, deciding an optimal strategy S_i requires the other players to play optimally too, so that social optimal equilibrium can be achieved. The optimization problem can be presented mathematically as the following:

$$\max_{I_i, l_i} U_i^{net}(S_i, S_{-i})$$
$$\max_{I_i, l_i} \left(\frac{(\Gamma + l_i - \mathcal{F}(L_{-i}))l_i}{\mathcal{F}(L_{-i})} + \mathcal{F}(L_{-i})\right) a_0 \log(1 + I_i) - \frac{(1+l_i)^{\beta_1} V_i}{(1+l_i)^{\beta_1} + (\mathcal{F}(L_{-i}))^{\beta_2}} - \zeta(l_i) - I_i - c_p \tag{7}$$

subject to the constraints

$$0 \le I_i \le \mathcal{B}_i \quad \text{and} \quad 0 \le l_i \le \mathcal{L}_i \quad \forall i \in \mathcal{N} \tag{8}$$

III. Game Analysis

In this section, we aim to analyze the above formulated non-cooperative game for extracting the possible equilibrium strategy profile when it is played simultaneously among the N players. Considering a N-firm scenario, where each of them tries to maximize the optimization problem given in Eqn. (7), it can be seen that when $I_i > 0$, the firms' discounted gain cannot be high if they free-ride on the received information from CYBEX. The framework ensures that when a firm abstains from sharing, the gain received from CYBEX decreases as free-riding is strongly discouraged in the system. Hence the greedy nature of a firm will never lead it to achieve a maximum reward. However, if it continuously increase the exchange of discovered information, there is a chance it will receive higher reward than the previous greedy scenario. The sample numerical analysis given in Fig. 1 shows the declining nature (blue plot) of utility when the firm tries to free-ride by decreasing its breach sharing value from 35 to 0 starting at step 6. However, if it would have shared truthfully, the payoff could have been more than the previous case as shown in the figure (red plot).

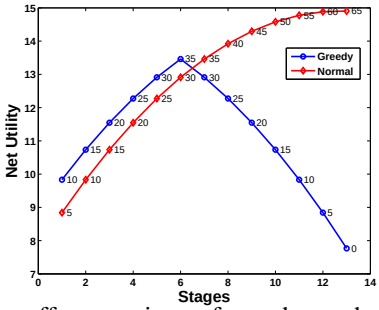

Fig. 1: Payoff comparison of greedy vs sharing nature

A. Existence of Nash Equilibrium

In this section we analyze the net utility expression of the firms to find a sufficient condition for the optimal values of security investment and information to share, such that the net payoff is maximized. This analysis will ensure the existence of socially-optimal equilibrium strategy for the firms, which will reward maximum provided every other firm plays with their best response strategies.

Lemma 3.1: A firm will never share anything, when its budget for security investment is null, i.e. the dominant NE strategy of the game will be to not share any information.

Proof: When a firm does not make any security investment, i.e. $I_i = 0$, then the gain component of net utility, as shown in Eqn. (7), is 0. Thus the net payoff is composed on only cost component, which will be maximized when the firm does not share anything ($l_i = 0$). Therefore, no sharing is the only Nash equilibrium in this scenario. Hence security investment is an important decision to make in the game, otherwise the framework will not be successful. ■

The following lemma proves the conditional existence of socially-optimal strategy profile that ensures the firms in maximizing their utility if they adhere to their corresponding optimal investment and amount of information to share.

Lemma 3.2: Socially-optimal strategy profile exists for the firm i if every firm invests I_i and truthfully share l_i breach related discoveries with CYBEX, such that the following condition is satisfied.

$p_i''V_i\mathcal{Z}^2 + \zeta''(l_i)\mathcal{Z}^2 - 2a_0\mathcal{Z}\log(1+I_i) - \frac{a_0(\mathcal{Z}\alpha_i+l_i)^2}{(\alpha_i l_i+\mathcal{Z})} > 0$
where, $\mathcal{Z} = \mathcal{F}(L_{-i})$

Proof: To prove the existence of socially-optimal strategy profile for the firm i's multi-parameter net utility function, we need to show that there exists a tuple of security investment (I_i) and amount of information to share (l_i) which will maximize the net utility given in (7). Hence we must show that U_i^{net} is strictly concave under the coupled constraint tuple (I_i, l_i). To prove the concavity nature in this game of couple constraints, we need to check whether the Hessian of U_i^{net} is negative definite. Now differentiating Eqn. (7) with respect to I_i, we find

$$\frac{\partial U_i^{net}}{\partial I_i} = \frac{a_0(\alpha_i l_i + \mathcal{F}(L_{-i})}{1+I_i} - 1 \tag{9}$$

Similarly, differentiating U_i^{net} with respect to l_i, we get

$$\frac{\partial U_i^{net}}{\partial l_i} = \frac{(\Gamma+2l_i-\mathcal{F}(L_{-i}))a_0\log(1+I_i)}{\mathcal{F}(L_{-i})} - p_i'V_i - \zeta'(l_i) \tag{10}$$

where $p_i' = \frac{\beta_1(1+l_i)^{(\beta_1-1)}(\mathcal{F}(L_{-i}))^{\beta_2}}{[(1+l_i)^{\beta_1}+(\mathcal{F}(L_{-i}))^{\beta_2}]^2}$ is the first order differential of the attack probability with respect to l_i and $\zeta'(l_i) > 0$ is assumed earlier.

The Hessian of U_i^{net} can be represented as:

$$\mathcal{H} = \begin{bmatrix} \frac{\partial^2 U_i^{net}}{\partial I_i^2} & \frac{\partial^2 U_i^{net}}{\partial I_i \partial l_i} \\ \frac{\partial^2 U_i^{net}}{\partial l_i \partial I_i} & \frac{\partial^2 U_i^{net}}{\partial l_i^2} \end{bmatrix} \tag{11}$$

Again differentiating the first order differentials given in Eqn. (9) and (10) with respect to I_i and l_i, then substituting in Eqn. (11), $\mathcal{H}$ can be re-written as,

$$\mathcal{H} = \begin{bmatrix} \frac{-a_0(\alpha_i l_i+\mathcal{F}(L_{-i}))}{(1+I_i)^2} & \frac{a_0(\Gamma+2l_i-\mathcal{F}(L_{-i}))}{(1+I_i)\mathcal{F}(L_{-i}))} \\ \frac{a_0(\Gamma+2l_i-\mathcal{F}(L_{-i}))}{(1+I_i)\mathcal{F}(L_{-i}))} & \frac{2a_0\log(1+I_i)}{\mathcal{F}(L_{-i}))} - p_i''V_i - \zeta''(l_i) \end{bmatrix} \tag{12}$$

where, assuming $\mathcal{Z} = \mathcal{F}(L_{-i})$, second order differential of p_i can be defined as:

$$p_i'' = \frac{\beta_1\mathcal{Z}^{\beta_2}(1+l_i)^{\beta_1-2}[(\beta_1-1)\mathcal{Z}^{\beta_2} - (\beta_1+1)(1+l_i)^{\beta_1}]}{[(1+l_i)^{\beta_1}+\mathcal{Z}^{\beta_2}]^3}$$

For $\mathcal{H}$ to be negative definite, the necessary and sufficient conditions are $\mathcal{H}_{11} = \frac{\partial^2 U_i^{net}}{\partial I_i^2} < 0$ and determinant of Hessian matrix must be positive, i.e. $\det(\mathcal{H}) > 0$. As it is obvious from Eqn. (12), $\frac{\partial^2 U_i^{net}}{\partial I_i^2} = \frac{-a_0(\alpha_i l_i+\mathcal{Z})}{(1+I_i)^2} < 0$, hence satisfies the first condition. Now, finding the determinant of $\mathcal{H}$:

$$\det(\mathcal{H}) = \frac{-a_0(\alpha_i l_i+\mathcal{Z})}{(1+I_i)^2}\left[\frac{2a_0\log(1+I_i)}{\mathcal{Z}} - p_i''V_i - \zeta''(l_i)\right] - \frac{a_0^2(\Gamma+2l_i-\mathcal{Z})^2}{(1+I_i)^2\mathcal{Z}^2} \tag{13}$$

The determinant given in Eqn. (13) will be positive at the optimal I_i^* and l_i^*, if the following condition is satisfied:

$$\frac{a_0(\mathcal{Z}\alpha_i+l_i^*)^2}{(\alpha_i l_i^*+\mathcal{Z})} < p_i''V_i\mathcal{Z}^2 + \zeta''(l_i^*)\mathcal{Z}^2 - 2a_0\mathcal{Z}\log(1+I_i^*)$$
$$\implies p_i''V_i\mathcal{Z}^2 + \zeta''(l_i^*)\mathcal{Z}^2 - 2a_0\mathcal{Z}\log(1+I_i^*) - \frac{a_0(\mathcal{Z}\alpha_i+l_i^*)^2}{(\alpha_i l_i^*+\mathcal{Z})} > 0 \tag{14}$$

To find the optimal value of the coupled constraint parameters of the firm i (I_i^*, l_i^*), we need to solve the first order differential equations given in Eqn. (9) and (10) by equating them to zero. The optimal values can be found out by solving the followings,

$$I_i^* = a_0(\alpha_i l_i^* + \mathcal{Z}) - 1 \tag{15}$$

$$p_i(l_i^*)'V_i + \zeta'(l_i^*) - \frac{(\Gamma+2l_i-\mathcal{Z})}{\mathcal{Z}}a_0\log(1+I_i^*) = 0 \tag{16}$$

The solutions of the above two coupled equation represent the optimal investment and sharing valuation, that constitute the socially-optimal strategy of player i. Hence the firms participating in the sharing framework will receive maximum utility if they play with their socially-optimal responses that follow the condition (14).

Given the condition (14) holds, it is clear that the Hessian $\mathcal{H}$ of U_i^{net} is negative definite. Thus it proves the strict

concavity nature of the utility function and the existence of socially-optimal equilibrium point for the coupled constraint optimization problem. ■

B. Guidance for CYBEX

As CYBEX coordinates the information exchange process among the participating corporations, its first and foremost goal is to self-motivate as many firms to participate in the sharing framework that will create a win-win situation for both the service-seeking firms as well as the CYBEX itself. Therefore, CYBEX requires a robust incentive model, which can help in motivating the firms to share if they truthfully exchange their discoveries, whereas punish them if they try to free-ride on others' shared information. A robust incentive model (α_i) for CYBEX is needed that can suitably reward/punish the firms depending on how they are contributing to the sharing framework. If a firm shares more information whereas other participating firms are not, then CYBEX rewards the former firm more to keep it motivated towards sharing. However, if it shares minimum and the rest of the firms have exchanged a large amount of information, then this is a case of free-riding of the former firm. In this situation, CYBEX rather punishes with low α_i value to prevent such information exploitation scenarios. The reward of sharing effectiveness value (α_i) is comparatively high when the overall system of participants are at the initial stages and need to be motivated to share more, whereas when the sharing system is stable and every firm is willing to share its security information truthfully, α_i can decrease to a lower value to let the sharing framework self-sustain. Based on the above characteristics, the following incentive model best fits for CYBEX's requirements and can be represented as:

$$\alpha_i = \frac{\Gamma + l_i - \mathcal{F}(L_{-i})}{\mathcal{F}(L_{-i})}$$

The following insights can be deduced to understand the physical significance of the above equation. When, the sharing amount (l_i) of firm i increases and other participants do not share a lot i.e. $\mathcal{F}(L_{-i})$ is low then the reward α_i provided by CYBEX is high, thus motivating the firm i to continue its sharing. However, when l_i is low, and $\mathcal{F}(L_{-i})$ is high, then firm i is trying to free-ride, and CYBEX rewards low α_i value to prevent such behavior.

IV. Results and Discussion

Here, we present the results obtained from numerical analysis and simulations to validate our cybersecurity information sharing model. To show the existence of socially-optimal equilibrium security investment and information sharing strategies of a firm, we used the net utility expression given in Eqn. (7). The regression parameters in the attack probability model are considered as: $\beta_1 = 5, \beta_2 = 3$. The reputation function, $\zeta(l_i)$ is considered to be a quadratic expression equivalent to $w_1 l_i^2$, where $w_1 > 0$. The received information set $\mathcal{F}(L_{-i})$ from CYBEX is assumed to be the total amount of information exchanged by other participating firms except i, thus $\mathcal{F}(L_{-i}) = \sum_{j \neq i} l_j$. For the experiment, we assume that each firm has total 25 information to share ($\mathcal{L}$) and has total budget ($\mathcal{B}$) of 350 to invest.

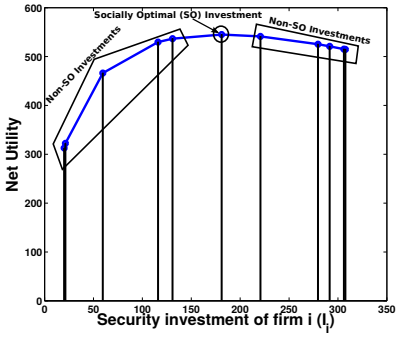

Fig. 2: Existence of Socially-Optimal Investment (I_i^*)

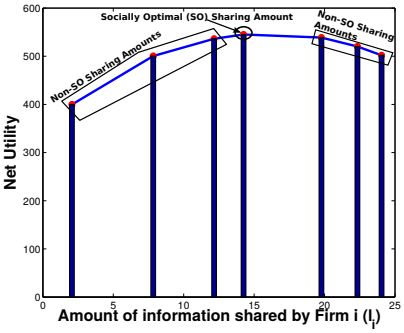

Fig. 3: Existence of Socially-Optimal sharing (l_i^*)

To prove the consistency of condition (14), we first find the feasible l_i and the corresponding $\mathcal{F}(L_{-i})$ numerically using Eqn. (16). Considering a single tuple $(I_i^*, l_i^*, \mathcal{F}(L_{-i}))$ that satisfies the condition (14), we tested whether this tuple is in fact the socially-optimal (SO) tuple by experimenting with different I_i and l_i values other than I_i^*, l_i^* respectively. In Fig. 2, we find that $I_i^* = 181.1$ value is the SO-strategy because (1) it satisfies the condition (14), (2) deviating from this investment and taking random investments below/above this value could not reward more. For this experiment, we keep the $l_i^*, \mathcal{F}(L_{-i})$ values fixed. Then we performed a similar experiment to verify, whether the optimal information sharing value ($l_i^* = 14.25$) is also a socially-optimal strategy or not by keeping $I_i^*, \mathcal{F}(L_{-i})$ values fixed. It is found from Fig. 3 that l_i^* that follows the condition (14), returns highest utility which cannot be achieved by other different l_i values. Therefore, it can be ensured that if the tuple $(I_i^*, l_i^*, \mathcal{F}(L_{-i}))$ satisfies condition (14), then it is a socially-optimal equilibrium strategy profile for firm i.

In order to understand the nature of investment of a firm i, where other participating firms share a fixed amount of information, we present a sample scenario in Fig. 4. It is noticed that there exists an optimal amount of information to be shared (l_i) at which the net utility is maximized for a particular investment quantity. It is also observed that the optimal sharing amount increases as the firms make higher security investment to discover more information. However, it is not true that a firm will receive larger payoff upon large investment, rather the cost component dominates over outcome

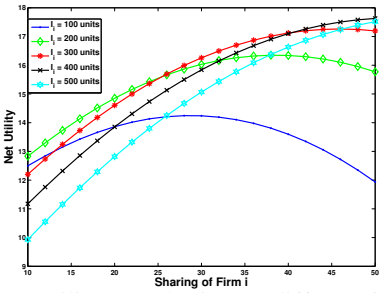

Fig. 4: Net utility vs. Sharing at different investment

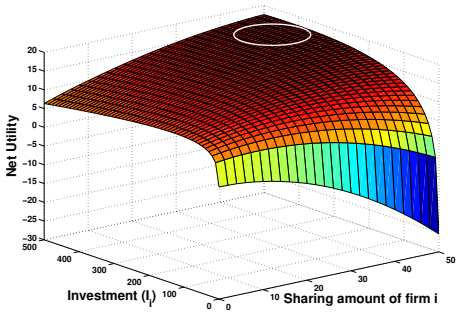

Fig. 5: Net utility variation at simultaneous optimization

of such huge investment after a certain threshold. From the plot, we see that the firm receives increasing reward when I_i is increased from 100 to 400. However, further increase in the investment amount does not increase the net utility any more. Thus it can be inferred that there exists an optimal peak investment limit beyond which the firms cannot gain high benefit. However, the optimal investment amount might vary depending on total number of security information received from CYBEX in that decision period.

In Fig. 5, the firm's investment and information sharing amount are varied simultaneously to verify the nature of net utility function. Assuming a total 50 units of vulnerability information shared by the other participating firms, it is found that the net payoff for firm i can be maximized for a particular strategy tuple (I_i^*, l_i^*), when it satisfies the condition given in Eqn. (14). This strategy profile lies in between the white circle on top of the curve presented in the figure (5) that corresponds to the maxima of the utility function. This proves the existence of the socially-optimal decision parameters for the current scenario that satisfy the derived condition in Section III.

V. Conclusions

In this research, we addressed the problem of cybersecurity related information sharing among various corporations to support them in building a robust and secure infrastructure in future. We pointed out the major concerns and factors that affect a corporation's decision to participate in the information exchange framework. Then we formulated a non-cooperative game between N firms who share their cybersecurity related information via CYBEX. We modeled this as an optimization problem by formulating a utility function for the firms and solved to find the socially-optimal equilibrium point, consisting of the tuple (amount of investment and quantity of information to share) that maximizes the firms' net reward. We presented the numerical results to verify the existence of the socially-optimal strategy profile and proposed guidance for CYBEX to motivate the firms towards actively participate and share in the framework. In future, we aim to study this game from an evolutionary game perspective by including possibility of malicious firms, where players can dynamically decide their strategies by learning from their past actions and eventually reach to an evolutionary stable strategy.

References

[1] http://www.huffingtonpost.com/2013/12/05/jpmorgan-cyber-attack_n_4388779.html.

[2] http://www.reuters.com/article/2013/03/13/us-jpmorgan-cyberattack-idUSBRE92C02520130313.

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

[4] http://www.businessinsider.com/apple-statement-on-icloud-hack-2014-9.

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

[6] K. Hausken, "Information sharing among firms and cyber attacks," *Journal of Accounting and Public Policy*, vol. 26, pp. 639–688, 2007.

[7] M. Kadivar, "Cyber-attack attributes," *Technology Innovation Management Review*, p. 22, 2014.

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

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

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

[11] 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

[12] http://fcw.com/articles/2014/08/06/what-keeps-darpa-up-at-night.aspx.

[13] 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.

[14] 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

[15] 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.

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

[17] W. Bossert and Y. Sprumont, "Non-deteriorating choice," *Economica*, vol. 76, no. 302, pp. 337–363, 2009.

[18] J. Apesteguia and M. A. Ballester, "A measure of rationality and welfare," *Working Papers (Universitat Pompeu Fabra. Departamento de Economía y Empresa)*, no. 1220, p. 1, 2010.

[19] 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.

[20] R. Litzenberger and M. Rubinstein, "The strong case for the generalized logarithmic utility model as the premier model of financial markets," *The Journal of Finance*, vol. 31, no. 2, pp. 551–571, 1976.

[21] L. L. Kupper, C. Portier, M. D. Hogan, and E. Yamamoto, "The impact of litter effects on dose-response modeling in teratology," *Biometrics*, pp. 85–98, 1986.

[22] P. Teunis and A. Havelaar, "The beta poisson dose-response model is not a single-hit model," *Risk Analysis*, vol. 20, no. 4, pp. 513–520, 2000.

[23] S. Anand, S. Sengupta, and R. Chandramouli, "An attack-defense game theoretic analysis of multi-band wireless covert timing networks," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9.

[24] M. H. Fleming and E. Goldstein, "Metrics for measuring the efficacy of critical-infrastructure-centric cybersecurity information sharing efforts," *Available at SSRN 2201033*, 2012.