# Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance

Deepak K. Tosh[1](✉), Iman Vakilinia[2], Sachin Shetty[3], Shamik Sengupta[2],
Charles A. Kamhoua[4], Laurent Njilla[5], and Kevin Kwiat[5]

[1] Department of Computer Science, Norfolk State University, Norfolk, VA, USA
dktosh@nsu.edu

[2] Department of Computer Science and Engineering,
University of Nevada, Reno, NV, USA
{ivakilinia,ssengupta}@unr.edu

[3] Virginia Modeling Analysis and Simulation Center,
Old Dominion University, Norfolk, VA, USA
sshetty@odu.edu

[4] Network Security Branch, Army Research Laboratory, Adelphi, MD, USA
charles.a.kamhoua.civ@mail.mil

[5] Cyber Assurance Branch, Air Force Research Laboratory, Rome, NY, USA
{laurent.njilla,kevin.kwiat}@us.af.mil

**Abstract.** Cyber-threat landscape has become highly complex, due to which isolated attempts to understand, detect, and resolve cybersecurity issues are not feasible in making a time constrained decisions. Introduction of cyber-threat information (CTI) sharing has potential to handle this issue to some extent, where knowledge about security incidents is gathered, exchanged across organizations for deriving useful information regarding the threat actors and vulnerabilities. Although, sharing security information could allow organizations to make informed decision, it may not completely eliminate the risks. Therefore, organizations are also inclined toward considering cyber-insurance for transferring risks to the insurers. Also, in networked environment, adversaries may exploit the information sharing to successfully breach the participating organizations. In this paper, we consider these players, i.e. organizations, adversary, and insure, to model a three layer game, where players play sequentially to find out their optimal strategies. Organizations determine their optimal self-defense investment to make while participating in CTI sharing and cyber-insurance. The adversary looks for an optimal attack rate while the insurer targets to maximize its profit by offering suitable coverage level to the organizations. Using backward induction approach, we conduct subgame perfect equilibrium analysis to find optimal strategies for the involved players. We observe that when cyber-insurance is not

Approved for Public Release; Distribution Unlimited: 88ABW-2017-3219, 05 Jul 2017. This work was supported by the Office of the Assistant Secretary of Defense for Research and Engineering (OASD (R&E)) agreement FA8750-15-2-0120, Department of Homeland Security Grant 2015-ST-061-CIRC01 and National Science Foundation (NSF), Award #1528167.

S. Rass et al. (Eds.): GameSec 2017, LNCS 10575, pp. 519–532, 2017.
DOI: 10.1007/978-3-319-68711-7_28

considered, attacker prefers to increase its rate of attack. This motivates the organizations to consider cyber-insurance option for transferring the risks on their critical assets.

**Keywords:** Cyber-insurance · Cyber-threat information sharing · Game theory · CYBEX

## 1 Introduction

Growing utilization of cyberspace invites malicious adversaries to exploit unpatched vulnerabilities of Internet users/organizations for various profitable reasons. The cyber attacks are becoming sophisticated and complex day by day, where the adversaries target the victims and persist until their objectives are pursued. Therefore, the attackers always try to stay one step ahead of victims and use advanced tactics, techniques, and procedures (TTPs) to achieve their goals. While it is becoming difficult for the cyberspace users to detect and prevent cyber-malicious activities using the traditional signature-based security measures, independent efforts to address such issues are turning out to be ineffective in practice. Due to this, security researchers, and policy makers are emphasizing on enforcing mutual collaborative efforts from private organizations and government institutions for collecting, sharing and analyzing threat information. This could help in deriving proactive cyber-intelligence [6] to efficiently identify structured information regarding novel attack campaigns, compromised resources, TTPs, actors behind the scene etc. and take defensive actions in a timely manner [4].

The significance of cybersecurity information sharing has lead governments and regulators to mandate/encourage such sharing. In U.S., the Cybersecurity Information Sharing Act (CISA) [1] bill motivates for collaborative sharing among private and public sector organizations by providing liability protections to the sharing parties. EU has also launched several cross-sector and intra-sector initiatives to enhance the EU Member States' capability for preparedness, cooperation, information exchange, coordination, and response to cyber threats. Furthermore, ITU-T has approved a CYBersecurity information EXchange (CYBEX) [16] framework that facilitates organization and sharing cyber-threat information, such as knowledge of threats, vulnerabilities, incidents, risks, and mitigations and their associated remedies.

On the other hand, the inescapable fact is that it is impossible to achieve perfect/near-perfect cybersecurity protection. Therefore, organizations also rely on cyber-insurance to transfer the cyber-related risks on their critical assets. Cyber-insurance is a risk management technique via which cyber-risks are transferred to an insurance company, in return for a periodic fee, i.e., the insurance premium. Cyber-insurance can indemnify various costs impacted from cyber-attacks causing data destruction, extortion, theft, hacking, and denial of service attacks. Although, insurance could indirectly improve security of an organization, it also demands investment on self-defense mechanisms. The possibility of correlated risks from other entities caused due to networked environment also hints to participate in collaborative CTI sharing. Having noticed the usefulness of CTI sharing and cyber-insurance, it is important to model the mutual interaction between organizations and insurer in presence of an adversary, where organizations opt for both risk mitigation approaches to maintain socially efficient security level.

In this work, we consider organizations, adversaries, and insurers as three category of players in the game with periodic strategic interactions. The organization aims to find its optimal self-defense investment while participating in information sharing and undertaking cyber-insurance. However, adversarial attacks negatively affect the organization, which also costs the adversary. Therefore, it requires an optimal and balanced attack rate that will cause maximum disruption to the organizations. At the same time, organizations consider cyber-insurance to protect their critical assets by paying a premium to the insurers, who provide a certain level of coverage on the event of a cyber-breach. Thus, the insurer aims to offer an optimal coverage level to the organizations so that both insured and insurer maximize their payoffs. We consider a sequential interaction of three players, starting with the organization who decides its self-defense investment, followed by the adversary who chooses the attack rate. Then, the insurer plays its strategy to decide what coverage level it must offer an organization by observing its self-defense investment and attacker's attack rate. The game repeats further with the same interactions. We rigorously analyze the model when insurance is not undertaken by the defending organizations and show that this situation is not beneficial for them as the attacker's optimal strategy is to increase its attack rate.

This paper is organized as follows: Sect. 2 presents brief overview on prior research works. The system model of the 3-layer game is described in Sect. 3. The utility models and game formulation is presented in Sect. 4. In the Sect. 5, we analyze the sequential interaction game to derive Stackleberg equilibrium. The numerical results are presented in Sect. 6. Finally, Sect. 7 concludes the paper.

## 2 Related Works

This topic has gained significant attention and is being investigated by government, policy makers, economists, non-profit organizations, industries, cybersecurity and network professionals with researches in this particular area still emerging [8,9,22]. Considering the need of cybersecurity information sharing, Gordon et al. [11] analyzed the economic (dis)advantages of this activity and derived its relationship with accounting aspects of an organization. Using game theoretic models, [18,19] prove that information exchange activity improves the social welfare as well as security level of the firms. Incentivization schemes for inducing sharing nature is discussed in [13,17,20]. Authors of [7] have proposed a game theoretic model to determine the IT security investment levels and compare it with the outcome of a decision theoretic approach that considers various components, such as vulnerability, payoff from investment etc. Authors of [10] applied functional dependency network analysis to model the attack propagation for a set of correlated organizations and analyze the sharing behaviors.

On the other hand, cyber-insurance market is emerging [15] due to the high occurrence of targeted cyber breaches over the years. However, the components such as interdependent security, correlated risks, and information asymmetries [3,5] make it challenging to model appropriate policies for the organizations. Nash equilibrium analysis and social optima concepts are applied to model security games in [12] that consider above three components into account and decide how investment can be used for both public good (protection) and a private good (insurance). Full insurance and partial insurance coverage models are proposed in [14] and study the impact of cooperation on self-defense investments. Another quantitative framework is proposed in [23] that applies optimization technique to provide suggestions to the network users and operators on investments toward cybersecurity insurance by minimizing the overall cyber risks. Sequential interaction of three player groups, when organization consider both strategies for risk management, is not undertaken in prior research. This paper particularly models this problem and solve for Stackleberg equilibria for the formulated game.

## 3 System Model

In this section, we define the players of the game and the interactions among the organizations and insurance vendors in presence of adversaries in the cybersecurity information sharing framework. These players: organizations, insurer, and adversary, interplay in the sharing system to achieve their objectives as briefed in the following.

- *Organizations* operate their business essentials with the use of network systems and hence they are vulnerable to data breaches, and service disruptions. So, minimizing the losses from the adversary's cyber attacks is primary focus of the organizations.
- *Insurers* are the entities or companies, who assess the cyber-risks of the organizations and formulate potential insurance policies to cover financial damages (fully or partially) at the occurrence of successful cyber attacks at a cost of periodic subscription fee in the form of premiums.
- *Adversaries* are the malice users, who always try to take advantage of the communication network and system loopholes in the organizations to perform data breaches. Furthermore, attackers look deep into the shared cyber-threat information among the organizations to exploit them with the gained knowledge.

### 3.1 System Overview

As described above, our system involves three categories of players, where organizations are considered to be interconnected with each other and runs similar applications for their operations. Thus, the attacker has opportunity to attack individual organizations directly or indirectly via exploiting some other organization. So, the loss for an organization on a successful attack event can have two different components, namely direct and indirect loss. To avoid such losses, organizations typically invest in self-defense. However, this strategy may not completely alleviate the chances of getting compromised. Therefore, the organizations participate in a threat information sharing framework, where they exchange vulnerability related information, such as patches, and fixes with each other, to foster their proactive defense abilities.

In addition to the strategies of self-defense investment and CTI sharing, organizations also prefer to transfer some of the risks to third parties via insuring their critical assets. Thus, insurance companies come into the picture, who directly interact with organizations to evaluate their risk factors and offer coverage for assets that are candidates of cyber-exploitation. Typical categories of cyber-insurance coverage includes critical data breach, business interruption, destruction of data/software, denial of service, ransomware etc. Since cyber-insurance has become a critical component of cybersecurity risk management, we consider insurance provider as a player in our game model and analyze the impact of insurance coverage on the investment decisions of organizations and attack rate of adversaries.

### 3.2 Threat Model

In our proposed game model, it is considered that the organizations are vulnerable to cyber-breaches and the adversary is rational in nature. With assumption that the adversary can observe the strategies undertaken by the organizations, it might alter its attacking strategy to maximize its profit. This observation can be partial or full depending on how it conducts the reconnaissance phase prior to the attack. In our model, we assume the attacker has complete information about the defending organization's strategies. The two important parameters for the defenders are self-defense investment as well as amount of threat-information sharing among each other, which have (in)direct impacts on the rational adversary's overall utility. If the investment toward self-defense is observed to be higher, then the attacker's probability of successfully compromising the organization may be low. While at the same time, we believe that if the threat related information sharing is improved in the system, it helps the participants to enhance their security practice based on the community knowledge. Thus, observing this information, the adversary's attack strategy will be different and its payoff will be impacted.

### 3.3 Model Description

In our model, we consider a set $\mathcal{N}$ of $n$ risk-averse and rational organizations that operate in a networked environment, who also participate in the cybersecurity information sharing process. The organizations may or may not cooperate in disclosing the investment information with each other because of competitive advantages, however they voluntarily share CTI information to proactively defend future cyber attacks. Considering the market existence for cyber-insurance and self-defense, organizations look forward to invest in both strategies to reduce their risks on cyber-exploitation.

We consider that each organization $i$ has a fixed portion $T$ of total assets that it tries to protect. For risk reduction, the organization $i \in \mathcal{N}$ chooses to invest in self-defense, which is represented as $s_i \in [0, 1]$ and each self-defense investment maps to a particular risk probability $p(s_i)$. It is intuitive to state that the probability function is decreasing with respect to $s_i$, hence it is assumed that $p(s_i)$ is continuous and twice differentiable, i.e. $p'(s_i) < 0$ and $p''(s_i) > 0$. Also, the probability diminishes to zero, when the investment reaches to very high quantity, i.e. $\lim_{s_i \to \infty} p(s_i) = 0$. Similarly, we assume that every organization $i$ involved in CTI information exchange shares $l_i \in [0, 1]$ amount of cybersecurity information voluntarily with the others. This knowledge to the adversary may help to use against other organizations in performing data breach or service disruptions. So, we define another risk probability $q(\{l_i : i \in \mathcal{N}\})$ with respect to sharing of threat information. It represents the probability of getting breached when the system participants share $L = \{l_1, l_2, \cdots l_n\}$ amount of information individually with each other. We consider that this sharing risk function depends on every organization's CTI sharing strategy because others' information brings new insights for an organization, while sharing own information may have adversarial impact. Hence, the characteristics of sharing based risk probability function $q(L)$ has following properties. For an organization $i$, $q(L)$ increases with increase in $l_i$, however it decreases when $l_j$ increases for any $j \neq i$. Thus, $\frac{\partial q}{\partial l_i} > 0$ and $\frac{\partial^2 q}{\partial l_i^2} < 0$, but for any $j \neq i$, $\frac{\partial q}{\partial l_j} < 0$ and $\frac{\partial^2 q}{\partial l_j^2} > 0$. Although this risk probability infers that the more information an organization shares, the probability of cyber incident increases, it is also noted that this risk goes down if other organizations also collaboratively exchange their threat knowledge.

Although organizations are vulnerable to direct attacks from the adversaries depending on their self-defense investment and information sharing, there exists the possibility of indirect risks because of other organizations in the same network. The probability of direct attack to an organization $i$ can be represented as: $\mathbf{P}^i_{dir} = 1 - (1 - p(s_i))(1 - q(L))$, where the second term defines the probability of not getting direct attack from investing $s_i$ amount in self-defense and sharing $L = \{l_i, l_{-i}\}$ amount of threat information. Considering the dissemination of threat information is perfect in nature, the probability of indirect risk $(\mathbf{P}^i_{ind})$ for an organization $i$ depends on its own self-defense investment as well as sharing strategy of every other firm. This indirect risk can be interpreted as, $\mathbf{P}^i_{ind}(s_{-i}, L, n) = 1 - \prod_{j \neq i}^{n}(1 - p(s_j))(1 - q(L))$, where, $s_{-i}$ is the vector of self-investment values of all organizations except $i$. Hence, the total risk probability of organization $i$ can be expressed as combination of both direct and indirect risk, $\mathbf{P}_i = \mathbf{P}^i_{dir} + (1 - \mathbf{P}^i_{dir})\mathbf{P}^i_{ind}$.

$$\mathbf{P}_i(S, L, n) = 1 - \prod_{k=1}^{n}(1 - p(s_k))(1 - q(L)) \tag{1}$$

We can notice that with increase in information sharing ($l_i$), $q(L)$ increases and the second component of Eq. 1 decreases, thereby $\mathbf{P}_i(S, L, n)$ increases. Whereas, if the self-defense investment increases, $p(s_i)$ decreases and hence, the overall risk probability decreases. This characteristics is expected for any candidate probability function that is used to model cyber risk. As we mentioned earlier that cyber risks may not be completely eliminated, organizations also prefer to transfer their risk to insurance vendors. We consider a coverage function $G(X) : \mathbb{R} \rightarrow \mathbb{R}$ that maps the loss $X$ to an organization due to cyber attack event to the appropriate coverage level to offer. The firm pays a premium of amount $M(\alpha)$ periodically depending on the coverage level offered by the insurer. For simplicity, we consider a linear function for the coverage: $G(X) = \alpha X$, where $\alpha \in [0, 1]$ is the coverage level for the organizations and we denote the insurance policy as $\{\alpha, M\}$. In the next section, we formulate the individual objectives for the three group of players.

In this paper, the interactions of the players are considered to be sequential and the state of organizations' security can be either *compromised* or *protected* depending on the attacker's strategy. As simultaneous interactions rarely occur in reality, periodic strategic [21] interaction is focused in this paper. We initiate the game from the organization's side, where it decides the amount of self-defense investment to make, then attacker plays its strategy of choosing the attack rate to maximize its impact, and then the insurer plays its strategy of coverage by assessing organizations' security state. While attackers look for periodic optimal attack strategies, the organizations seek to find the right self-defense investment to make so that net payoff can be maximized.

# 4 Game Formulation

In the periodic interaction game, we assume that $z$ is the number of times an organization is at compromised state, i.e. $(1-z)$ times on average it is protected by its self-defense and CTI sharing. Considering the adversary attacks the organizations at a rate $\theta_a$ and organizations' defense rate is $\psi$, the mean value of $z$ [21] can be:

$$\mathbb{E}(z) = \begin{cases} 1 - \frac{\psi}{2\theta_a} & \text{if } \theta_a \geq \psi \\ \frac{\theta_a}{2\psi} & \text{Otherwise} \end{cases} \tag{2}$$

## 4.1 Organization's Payoff Model

Given the organization $i$ invests $s_i$ towards self-defense and shares $l_i$ amount of information with CYBEX, while other organizations share $l_{-i}$ amount, $i$'s net payoff model involves two components. First it gets rewarded from the security investment by a factor $I(s_i)$ and from others' shared information $B(l_{-i})$. Second, the loss protection by taking cyber-insurance coverage level $\alpha$. However, the costs involved are: (1) insurance premium $(M)$, which is a function of coverage level, and (2) cost of defending at rate $\psi$. By combining all the components, the net payoff of organization $i$ can be:

$$U_i(s_i, \theta_a, \{\alpha, M\}) = (1-z)I(s_i)B(l_{-i}) + z\alpha\mathbf{P}_iT - \psi C_d(s_i) - M(\alpha) \quad (3)$$

where, the first component is the estimated benefit out of self-investment and information sharing, when the organization is at protected state. The second component is the gain out of insurance coverage on the asset of value $T$. We can observe here that with higher coverage level, the expected gain $(z\alpha\mathbf{P}_iT)$ of an organization improves because it does not lose the total value of assets upon any cyber incident, rather a fraction of $T$ depending on what coverage the organization has opted for. The third component represents the cost of defending, where, $C_d(.)$ is the cost of each defense which depends on the self-defense investment. Finally, the last component is the premium cost that is dependent on the coverage level undertaken.

### 4.2 Adversary Payoff Model

The strategy of the adversary is to suitably vary its attack rate $(\theta_a)$ to cause maximum disruption to the organization by driving it to the compromised state. Thus, the attacker's benefit lies in average number of times the organization $i$ is at compromised state, i.e. $z$. However, it involves a cost $C_a$ to perform attack. Furthermore, the payoff is considered to decline as the information exchange activity and self-defense investment of organization $i$ are increased, which forms the third component of Eq. 4.

$$U_a(s_i, \theta_a, \{\alpha, M\}) = z - C_a\theta_a - (1-l_i)^b I(s_i) \quad (4)$$

where, $b \geq 1$ is an exponent to define the relevancy of information for the adversary.

### 4.3 Insurance Vendor's Payoff Model

The insurer's utility typically depends on the periodically collected premium amount $(M(\alpha))$. Whereas, the insurer must have to pay the coverage amount when an organization is affected due to cyber-breach, which constitutes the cost component of the insurance vendor and expressed in the following.

$$U_{Ins}(s_i, \theta_a, \{\alpha, M\}) = nM(\alpha) - \alpha\mathbf{P}_izT \quad (5)$$

## 5 Equilibrium Analysis

Considering the three group of players interacting sequentially in the system, we study the subgame perfect equilibrium under two different cases: (1) no cyber-insurance coverage is considered, and (2) in presence of insurance. In both cases, the organization first decides its self-defense investment at the starting of the game interaction, after which the adversary observes the actions taken by the organization and finds it optimal attack rate by maximizing its objective. If the organization have considered the cyber insurance for its risk transferring process, then the insurance vendor observes the prior actions played by the organization and the adversary to decide the optimal coverage level to recommend the organization along with its revised premium for the next interaction period in the game. Now, depending on the rate of attack by adversary and defense rate of the organization, we derive the subgame perfect equilibrium of our periodic interaction game.

### 5.1 No Cyber-Insurance Scenario

As the periodic interaction game, consisting of three group of players, modeled in the previous scenario mimics the characteristics of a sequential game, finding subgame perfect equilibrium will give more insights on the players' stable strategy. In the first scenario, we plan to analyze the game with consideration that the organizations are skipping cyber-insurance to avoid premium cost. Hence, $\alpha = 0$ in the organization $i$'s payoff model as presented in Eq. 3. Thus, the organization $i$ and attacker's payoff will be simplified as:

$$U_i(s_i, \theta_a) = (1 - z)I(s_i)B(l_{-i}) - \psi C_d(s_i) \tag{6}$$

$$U_a(s_i, \theta_a) = z - C_a\theta_a - (1 - l_i)^b I(s_i) \tag{7}$$

**Theorem 1.** *Given the adversary's attack rate is higher than organization's rate of defense and linear investment model, $I(s_i) = ks_i$, the Subgame Perfect Nash Equilibrium (SPNE) strategy for the organization-adversary game without the insurer is $(s_i^*, \theta_a^*)$.*

$$(s_i^*, \theta_a^*) = \begin{cases} \left(\frac{kB(l_{-i})C_d'^{-1}\sqrt{\widehat{K}}}{\sqrt{8C_a}}, \psi\right) & \textit{if } \psi(\psi^2 + 1) \geq 2C_a \\ \left(\frac{kB(l_{-i})C_d'^{-1}\sqrt{\psi+\widehat{K}}}{\sqrt{8C_a}}, \frac{\sqrt{2C_a}}{\sqrt{\psi+\widehat{K}}}\right) & \textit{Otherwise} \end{cases}$$

*where,* $\widehat{K} = k^2(1 - l_i)^b B(l_{-i})C_d'^{-1}$.

*Proof.* Considering, $\theta_a \geq \psi$, the mean value of $z$ is $1 - \frac{\psi}{2\theta_a}$ and replacing it in Eq. 6, the net payoff of organization $i$ is $U_i(s_i, \theta_a) = \frac{\psi}{2\theta_a} ks_iB(l_{-i}) - \psi C_d(s_i) - M(\alpha)$. Since, organization plays first it would try to find its optimal $s_i$ by maximizing Eq. 6. Thus, differentiating $U_i(s_i, \theta_a)$ w.r.t. $s_i$, we have, $\frac{\partial U_i}{\partial s_i} = \frac{\psi kB(l_{-i})}{2\theta_a} - \psi C_d'(s_i)$. Since cost of defense is always positive and an increasing function, it is easy to see that $\frac{\partial^2 U_i}{\partial s_i^2} < 0$. Thus, there exists an optimal self-defense investment $s_i^*$, which can be represented as $\frac{kB(l_{-i})C_d'^{-1}}{2\theta_a}$, where $C_d'^{-1}$ is the inverse first order differential of defense cost function. Now, the adversary's payoff becomes $1 - \frac{\psi + k^2(1-l_i)^b B(l_{-i}) C_d'^{-1}}{2\theta_a} - C_a\theta_a$, which is maximized at $\theta_a^* = \max\left\{\psi, \sqrt{\frac{2C_a}{\psi + \widehat{K}}}\right\}$. Now, if $\theta_a^* = \psi$, then attacker's payoff is $U_a = 0.5 - C_a\psi - \frac{\widehat{K}}{2\psi}$, which will be maximum only when $\psi = \sqrt{\frac{2C_a}{\widehat{K}}}$. Thus, $\psi^2 \geq \frac{2C_a}{\psi + \widehat{K}}$, due to which $\theta_a^* = \psi$. In other cases, adversary's payoff will be less than the above best-response. Therefore, the subgame perfect Nash equilibrium in this case will be $\left(\frac{k^2(B(l_{-i})C_d'^{-1})^{3/2}(1-l_i)^{b/2}}{\sqrt{8C_a}}, \psi\right)$. If $\theta_a^* = \sqrt{\frac{2C_a}{\psi + \widehat{K}}}$, the adversary payoff will be $U_a = 1 - \frac{(\psi + \widehat{K})^{1.5}}{\sqrt{8C_a}} - \frac{\sqrt{8C_a}}{\sqrt{\psi + \widehat{K}}}$. This scenario happens only if $\psi < \sqrt{\frac{2C_a}{\psi + \widehat{K}}}$ and the attacker will achieve maximum at a particular value of defense rate $\psi = \frac{8}{3}C_a - \widehat{K}$. Therefore, the subgame perfect equilibrium in this case will be $\left(\frac{kB(l_{-i})C_d'^{-1}\sqrt{\psi + \widehat{K}}}{\sqrt{8C_a}}, \sqrt{\frac{2C_a}{\psi + \widehat{K}}}\right)$.

## 5.2 Undertaking Cyber-Insurance

In this scenario, we consider the presence of insurer in the game and organizations undertake insurance coverage to reduce risk of cyber-loss. The insurer tries to find out the optimal insurance level to offer the organizations. In order to find the subgame perfect equilibrium of the three layer game between organizations, adversary, and insurer, we use backward induction approach. The interactions among players occur in the following manner: (i) first the organizations decide their self-defense investment ($s_i$), (ii) by observing this action of organizations, the adversary tunes its attack rate ($\theta_a$) for the considered stage, (iii) finally, by observing the strategies of organization's self-defense investment and the adversary's attack rate, the insurer decides what coverage level to offer the organizations. In our model, the organizations are considered to be homogeneous and share similar characteristics. The backward induction procedure is given below.

1. Organization $i$ finds investment $s_i(\theta_a, \alpha) = \text{argmax}_{s_i} U_i(s_i, \theta_a, \{\alpha, M\})$ for any $\theta_a$, $\alpha$.
2. After replacing $s_i(\theta_a, \alpha)$ in the attacker's payoff, it determines its attack rate, $\theta_a(\alpha) = \text{argmax}_{\theta_a} U_a(s_i(\theta_a, \alpha), \theta_a, \{\alpha, M\})$, for any $\alpha$.
3. Now, the insurer finds coverage $\alpha^* = \text{argmax}_{\alpha} U_{Ins}(s_i(\theta_a(\alpha), \alpha), \theta_a(\alpha), \{\alpha, M\})$.
4. Find the attacker's optimal attack rate $\theta_a^* = \theta_a(\alpha^*)$ and organization $i$'s optimal investment $s_i^* = s_i(\theta_a^*, \alpha^*)$, which form the SPNE $(s_i^*, \theta_a^*, \alpha^*)$ for our proposed three layer game.

**Proposition 1.** *Assuming a 2-organization and an opportunistic attack scenario, where the cost of defense is linear and rate of attack is higher than defense rate, the optimal security investment function for organization* 1 *is the following.*

$$s_1(\theta_a, \alpha) = \sqrt{\frac{(2\theta_a - \psi)(1 - p(s_2))(1 - q(L))tvT\alpha}{\psi(2\theta_a - kl_2)}} - \epsilon \tag{8}$$

*Proof.* In an opportunistic attack scenario, the probability of breach as a function of self-defense investment can be modeled [2] as $p(s_i) = \frac{tv}{s+\epsilon}$, where $\epsilon \ll 1$, and $v \in (0,1)$ is organization's intrinsic vulnerability, and $t$ is affinity factor to receive a particular type of attack. Also, when $\theta_a > \psi$, $z = 1 - \frac{\psi}{2\theta_a}$. Thus, organization 1's payoff can be rewritten as, $U_1(s_1) = \frac{\psi}{2\theta_a} k s_1 l_2 - \left(1 - \frac{\psi}{2\theta_a}\right) T\alpha(1 - \prod_{i=1}^{2}(1 - p(s_i))(1 - q(L))) - \psi C_d(s_1) - M(\alpha)$. The first order differential of above expression, by replacing $C_d(s_1) = s_1$, will be $U_1'(s_1) = \frac{\psi}{2\theta_a} kB(l_{-i}) + \left(1 - \frac{\psi}{2\theta_a}\right) T\alpha p'(s_1)(1 - q(L))(1 - p(s_2)) - \psi$, where $p'(s_1) = \frac{-vt}{(s_1+\epsilon)^2}$. Thus the optimal self-defense investment function $s_1(\theta_a, \alpha)$ can be obtained by solving $U_1'(s_1) = 0$, or $\psi(1 - \frac{kl_2}{2\theta_a}) = (1 - \frac{\psi}{2\theta_a})(1 - p(s_2))(1 - q(L))\alpha \frac{vt}{(s_1+\epsilon)^2}$, which gives rise the expression presented in Eq. 8. Using similar analysis, we can also derive the optimal self-defense investment function, $s_2(\theta_a, \alpha)$ for organization 2.

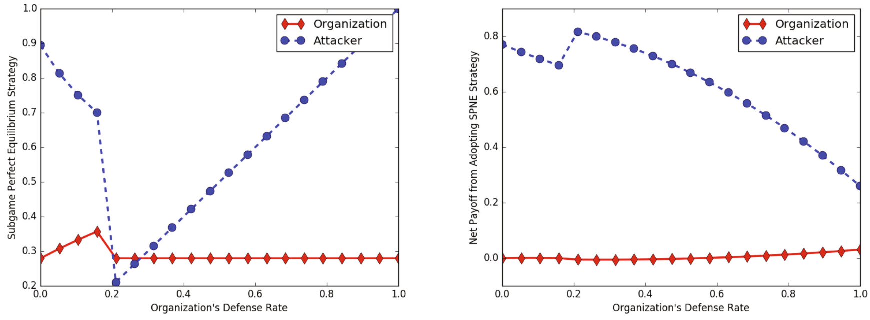
**Observations:** From the Eq. 8, we can observe that optimal self-defense investment is a function of attacker's as well as insurer's strategy. As the attacker's attack rate increases, the self-defense investment also needs to be updated accordingly in order to reduce the impact. Similarly, as the insurance level is higher, it demands to have more self-defense investment in order to keep harden the security, which can be inferred from Eq. 8 that $s_i \propto \sqrt{\alpha}$.

**Finding optimal attack rate and coverage level:** Now after deriving the optimal self-defense investments for both organizations, the attacker will tune its corresponding attack rates for maximizing the impact. So, to find the optimal rate of attack, $s_i(\theta_a, \alpha), i = 1, 2$ can be replaced in attacker's payoff model before solving for $\theta_a^*$. Considering the case of $\theta_a > \psi$, the payoff of attacker becomes, $U_a(\theta_a, \alpha) = (1 - \frac{\psi}{2\theta_a}) - C_a\theta_a - (1 - l_i)^b k s_i(\theta_a, \alpha)$. Thus, to find attack rate function $\theta_a(\alpha)$, the first order differential of $U_a$ must be equated to zero and solve, which leads to $U_a'(\theta_a, \alpha) = \frac{\psi}{2\theta_a^2} - C_a - (1 - l_i)^b \frac{\partial s_i}{\partial \theta_a} = 0$. The optimal attack rate must satisfy the condition $\frac{\psi}{2\theta_a^2} = C_a + (1 - l_i)^b \frac{\psi - kl_2}{\sqrt{2\theta_a - \psi}(2\theta_a - kl_2)^{1.5} C_0}$, where $C_0 = \sqrt{\frac{(1-p(s_2))(1-q(L))tvT\alpha}{\psi}}$. After finding $\theta_a(\alpha)$, the insurer's payoff needs to be maximized to find optimal coverage level, i.e. $\underset{\alpha}{\operatorname{argmax}} \{2M(\alpha) - \alpha T \sum_{i=1}^{2}((1 - \frac{\psi}{2\theta_a(\alpha)}))\mathbf{P}_i(s_i((\theta_a(\alpha), \alpha)))\}$. Finding a close form expression is difficult in this situation, which therefore needs to be solved numerically and we plan to extend this in our future work.

## 6 Numerical Results and Discussion

In this section, we evaluate our game theoretic model numerically to verify the existence of subgame perfect Nash equilibrium that we found earlier theoretically. To conduct the experiments, we consider two connected organizations and one adversary in the system, where sharing amount from each is fixed to 0.5. It is also assumed that the information dissemination is perfect and shared CTI information are not corrupted by the adversary. Information relevancy coefficient $b$ is fixed as 1. Since our model parameters are normalized between 0 and 1, a quadratic function is used to model the organization's cost of defense, $C_d(.)$, thus, $C_d' > 0$. The cost of attack $(C_a)$ is kept constant throughout the experiments as 0.1. We have varied the defense rate parameter of the organization to observe the strategic differences and the impacts on overall payoffs of both the organization as well as adversary. This scenario does not involve insurer.

In Fig. 1(a), we present the strategy landscape of both players for different possible defense rates of the organization. It is observed that adversary prefers to increase its attack rate at equilibrium when it observes the rate of defense is increasing beyond a certain threshold, which is 0.2 in our simulation instance. However, below this threshold the adversary's optimal attack rate decreases because of strategy reversal as derived in Theorem 1. For the considered parameter set, the optimal equilibrium strategy of both players change at $\psi = 0.2$, because the corresponding condition $\psi(\psi^2+1) \geq 2C_a$ is satisfied. We can observe this trend in Fig. 1(b), which represents the payoff variation of both players under the same circumstances. The adversary's net payoff decreases beyond this threshold because the optimal attack rate increases which involves cost $C_a$ for every attack. On the other hand, the organization's payoff increases slowly as its defense rate is increased. This is because the optimal investment in this phase has not changed. Before the strategy reversal point $\psi = 0.2$, the payoff of organization was decreasing due to their low investment. The take-away is that under no-insurance situation, attacker will prefer to raise its attack rate irrespective of organization's self-defense investment strategy. Thus, it motivates the organizations to consider the cyber-insurance option to improve their security standards.



(a) (b)

**Fig. 1.** (a) Subgame perfect equilibrium strategy w.r.t. organization's defense rate, (b) SPNE Payoff w.r.t. organization's defense rate

## 7 Conclusions and Future Research

The initiative to share cyber-threat information for addressing critical cybersecurity issues is important but it may not completely eradicate the possibilities of uncertain losses. Cyber-insurance is an alternative to transfer such risks to insurers. In this paper, we model a three layer game among organizations, adversary, and insurer to study the best decision strategy of self-defense investment for organizations, optimal attack rate for adversary and optimal coverage level for insurers. Modeling the interactions as sequential form, we used backward induction to solve for subgame perfect equilibrium the involved players. Numerical results show that attacker's prefer to increase their attack rate when the organization's defense rate is increased. In future, we plan to extend this research to find insights when the insurer plays before of the attacker and analyze the model for deriving optimal coverage level from the insurer's perspective.

## References

1. Cybersecurity information sharing act (cisa). https://www.congress.gov/bill/114th-congress/senate-bill/754
2. Huang, C.D., Behara, R.S.: Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. Int. J. Prod. Econ. **141**(1), 255–268 (2013)
3. Anderson, R., Moore, T.: The economics of information security. Science **314**(5799), 610–613 (2006)
4. Barnum, S.: Standardizing cyber threat intelligence information with the structured threat information expression (stix). MITRE Corporation 11 (2012)
5. Böhme, R., Schwartz, G., et al.: Modeling cyber-insurance: towards a unifying framework. In: WEIS (2010)
6. Burger, E.W., Goodman, M.D., Kampanakis, P., Zhu, K.A.: Taxonomy model for cyber threat intelligence information exchange technologies. In: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, pp. 51–60. ACM (2014)
7. Cavusoglu, H., Raghunathan, S., Yue, W.T.: Decision-theoretic and game-theoretic approaches to it security investment. J. Manage. Inf. Syst. **25**(2), 281–304 (2008)
8. Dandurand, L., Serrano, O.S.: Towards improved cyber security information sharing. In: 5th International Conference on Cyber Conflict, pp. 1–16. IEEE (2013)
9. de Fuentes, J.M., González-Manzano, L., Tapiador, J., Peris-Lopez, P.: Pracis: privacy-preserving and aggregatable cybersecurity information sharing. Comp. Secur. **69**, 127–141 (2016)
10. Garrido-Pelaz, R., González-Manzano, L., Pastrana, S.: Shall we collaborate?: a model to analyse the benefits of information sharing. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, pp. 15–24. ACM (2016)
11. Gordon, L.A., Loeb, M.P., Lucyshyn, W.: Sharing information on computer systems security: an economic analysis. J. Account. Public Policy **22**(6), 461–485 (2003)
12. Grossklags, J., Christin, N., Chuang, J.: Secure or insure?: a game-theoretic analysis of information security games. In: Proceedings of the 17th international conference on World Wide Web, pp. 209–218. ACM (2008)

13. Khouzani, M.H.R., Pham, V., Cid, C.: Strategic discovery and sharing of vulnerabilities in competitive environments. In: Poovendran, R., Saad, W. (eds.) GameSec 2014. LNCS, vol. 8840, pp. 59–78. Springer, Cham (2014). doi:10.1007/978-3-319-12601-2_4
14. Pal, R., Golubchik, L.: Analyzing self-defense investments in internet security under cyber-insurance coverage. In: 2010 IEEE 30th International Conference on Distributed Computing Systems (ICDCS), pp. 339–347. IEEE (2010)
15. Pal, R., Golubchik, L., Psounis, K., Hui, P.: Will cyber-insurance improve network security? a market analysis. In: INFOCOM, 2014 Proceedings IEEE, pp. 235–243. IEEE (2014)
16. Rutkowski, A., et al.: Cybex: the cybersecurity information exchange framework (x. 1500). ACM SIGCOMM Comput. Comm. Rev. **40**(5), 59–64 (2010)
17. Tosh, D.K., Sengupta, S., Kamhoua, C.A., Kwiat, K.A., Martin, A.: An evolutionary game-theoretic framework for cyber-threat information sharing. In: IEEE International Conference on Communications, ICC, pp. 7341–7346 (2015)
18. Tosh, D.K., Sengupta, S., Mukhopadhyay, S., Kamhoua, C., Kwiat, K.: Game theoretic modeling to enforce security information sharing among firms. In: IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 7–12 (2015)
19. Vakilinia, I., Sengupta, S.: A coalitional game theory approach for cybersecurity information sharing. In: Military Communications Conference, (MILCOM). IEEE (2017)
20. Vakilinia, I., Tosh, D.K., Sengupta, S.: 3-way game model for privacy-preserving cybersecurity information exchange framework. In: Military Communications Conference, (MILCOM). IEEE (2017)
21. Van Dijk, M., Juels, A., Oprea, A., Rivest, R.L.: Flipit: the game of "stealthy takeover". J. Cryptol. **26**(4), 655–713 (2013)
22. Wang, T., Kannan, K.N., Ulmer, J.R.: The association between the disclosure and the realization of information security risk factors. Inf. Syst. Res. **24**(2), 201–218 (2013)
23. Young, D., Lopez, J., Rice, M., Ramsey, B., McTasney, R.: A framework for incorporating insurance in critical infrastructure cyber risk strategies. Int. J. Crit. Infrastruct. Prot. **14**, 43–57 (2016)