A Coalitional Cyber-Insurance Framework for a Common Platform

Iman Vakilinia, Shamik Sengupta

Abstract—Despite the benefits of cyber-insurance, organizations are reluctant to enroll in such policies mainly because of their limitation and high price. On the other hand, insurers are confronting the adverse selection and moral hazard problems as monitoring and distinguishing insureds' cybersecurity posture are highly complicated. Considering the organizations' security interdependency and their demand for cyber-insurance, we study the design of coalitional insurance mechanisms with the goal of covering the adverse selection, moral hazard, and motivating players for cybersecurity investment and information sharing. To this end, we propose a synergistic insurance framework where organizations collaboratively insure a common platform instead of themselves. We present three models for insuring a common platform. In the first model, organizations act as both insurer and insured to distribute the risk in the coalition. In the second model, the system provides rewards to crowdfund the insurance. Finally, in the third model, we investigate the outsourcing of a common platform insurance. Furthermore, we discuss how our proposed mechanisms for such framework satisfy the budget balanced, *ex ante* individual rationality, and incentive compatibility properties. We study how such a system can improve the social welfare by leveraging cyber-insurance as a motivation for organizations to cooperate on the cybersecurity investment and information sharing.

Index Terms—Cyber-Insurance, Interdependent Security, Cybersecurity Information Sharing

1 Introduction

Due to the growing dependency on cyberspace, businesses in different domains invest in cybersecurity to safeguard their IT assets from cyber-threats. In spite of the necessity of having security measures, they are not sufficient to detect/prevent zero-day and sophisticated cyber-attacks. As a result, organizations are enduring massive damages caused by attackers. Since organizations cannot completely mitigate cyber-threats, they adopt cyber-insurance to transfer such risks to another party known as the insurer. It is estimated that annual gross written premium will be increased from around $\$2.5$ billion today to reach $\$7.5$ billion by 2020 [1].

However, several challenges are circumventing the growth of the cyber-insurance market. For instance, the lack of reliable data to compute insurance premium, and legal and procedural hurdles for assessing the organizations' security posture are two of them [2]. In addition, setting a proper insurance policy and premium is sophisticated. If the insurance policy is loose, the insurer might fail or even may go bankrupt, and if the policy is strict, the insured might withdraw from the contract and accept the risks. Moreover, asymmetric information between the insurer and insured exacerbates the situation causing moral hazard and adverse selection problems [3], [4]. Moral hazard refers to the case where insureds can increase the probability of the risks after signing the contract. For instance, the insured reduces its security investment after signing the insurance contract. On the other hand, users with high risk are more likely to take insurance, and an insurer cannot distinguish between insureds before signing the contract. This problem is known as adverse selection.

As the organizations are using the same software libraries, operating systems, firmware, applications, and hardware, they are susceptible to a common set of vulnerabilities. For instance, consider the Heartbleed vulnerability (CVE-2014-0160) in the OpenSSL library which was disclosed on April 2014 [5]. Heartbleed is a severe memory handling bug that results from improper input validation, which allows an attacker to steal the servers' data that includes private keys, users' session cookies, and passwords. It is estimated that around half a million of the secure web servers on the Internet certified by trusted authorities were vulnerable to the Heartbleed at the time of disclosure. This vulnerability affected other network services such as email servers, VPNs, and network appliances which were applying the OpenSSL library in their implementation [6].

Since organizations using the common platforms are suffering from the same set of vulnerabilities, their security is interdependent. In this situation, as one party's investment on security and detection of a common platform's vulnerabilities brings the positive externalities to other parties using the same platform, organizations tend to under-invest on security, expecting other organizations' investment [7], [8].

Besides that, organizations using the same platform can reduce the damages of attacks by sharing their cybersecurity information. However, sharing such information is costly for organizations. For instance, reporting a successful cyber-attack may affect the organizations' reputation negatively while such information can help other organizations to patch their systems to be safe from the same type of attack. Therefore, organizations tend to free-ride by taking advantage of the shared information while not reciprocating. In other words, if we model the cybersecurity information sharing as a non-cooperative game, although the sharing strategy is the socially optimal point, the not-sharing behavior is the Nash-Equilibrium point [9].

Therefore, it is important to motivate organizations to cybersecurity investment and sharing cybersecurity information. Such motivation can be done by assigning punishment/reward to the organizations. However, designing such mechanisms is a big challenge mainly because the provisioning of the cybersecurity investment and sharing is difficult.

- *This research is supported by the National Science Foundation (NSF), USA, Award #1528167.*

- *Iman Vakilinia and Shamik Sengupta are with the Department of Computer Science and Engineering, University of Nevada, Reno, NV, 89557. E-mail: ivakilinia@unr.edu, ssengupta@unr.edu*

Considering the organizations' security interdependency and their demand for cyber-insurance, we study the design of coalitional insurance mechanisms with the goal of covering the adverse selection, moral hazard, and cybersecurity investment and sharing problems. To this end, we propose a synergistic insurance framework where organizations collaboratively insure a common platform instead of themselves. We present three models for insuring a common platform. In the first model, organizations act as both insurer and insured to distribute the risk in the coalition. In the second model, the system provides rewards to crowdfund the insurance. Finally, in the third model, we investigate the outsourcing of a common platform insurance. Moreover, we study how such frameworks can improve social welfare by motivating organizations to collaborate on the cybersecurity investment and sharing.

The main contributions of this work are the two parts, as described below.

1- We propose a coalitional insurance framework where organizations act as both insurer and insured of a common platform. Further, we discuss how our proposed mechanisms for such framework satisfy the budget balanced, *ex ante* individual rationality, and incentive compatibility properties.

2- We present a model for crowdsourcing the insurance of a common platform taking into account the budget balanced, *ex ante* individual rationality, and incentive compatibility to propel organizations toward social welfare.

To the best of our knowledge, this work is the first to investigate the coalitional cyber-insurance framework for a common platform. This framework is applicable to other public-good insurance use-cases as well since the players can act as both insured and insurer at the same time for the public-good.

The rest of the paper is organized as follows. The next section reviews major works in interdependent security, cyber-insurance, and cybersecurity information sharing. In section 3, we introduce our system model. Details of our proposed mechanisms are described in section 4. The numerical results have been discussed in section 5. Finally, we conclude our paper in Section 6.

2 Related Work

2.1 Interdependent Security

An organization's security effort to find a vulnerability for a common platform brings positive externality to other organizations using the same platform. Game theory has been extensively applied to model such security interdependency between strategic users [10]–[17]. In such games, the players' goal is to minimize the security risk and the security investment cost altogether. In this case, players under-invest in security expecting other players investment. This problem is known as free-riding [12]. This causes a general under-investment in security and as a result, the security risks increase.

Price of Anarchy is the ratio between the Nash equilibrium and the social optimum and it specifies how a system's inefficiency grows because of selfish behavior of its players. Authors in [13] have demonstrated that the *Price of Anarchy* in the strategic-form of interdependent security systems increases with the increase in the number of agents and their interdependency. Naghizadeh *et al*. in [15] have studied the impossibility of designing a mechanism for interdependent security games which fulfills the social optimality, voluntary participation, and the weak budget balanced properties altogether. Böhme [16] has studied the role of auditing in improving utility in the interdependent security games. Farhadi *et al*. [17] have studied a dynamic incentive mechanism design problem in networks of interdependent strategic agents. Their proposed dynamic mechanism aims to maximize social welfare while satisfying the expected individual rationality and the budget balanced properties. Xiao *et al*. [14] have proposed a security model based on the indirect reciprocity principle to detain wireless nodes from adversary behavior.

Considering these works, in this paper, we propose mechanisms to improve the overall security in an interdependent setting by exploiting the coalition of players for insuring a common platform.

2.2 Cyber-Insurance

The design of a cyber-insurance contract has been studied extensively in the literature [2]–[4], [18]–[27]. Johnson *et al*. [2] have formulated a one-shot security game with market insurance assuming homogeneous players, fair insurance premiums, and complete information. The result of this research demonstrates the importance of tuning the stipulations for security investment and the development of a market for cyber-insurance to achieve social welfare. The role of cyber-insurance in improving the overall security has been studied in [22], [24]. Pal *et al*. [22] have shown that in the oligopolistic cyber-insurance market, the network security is not improving. However, a monopoly cyber-insurer can help solve the moral hazard problem partially and improve network security by discriminating the contracts.

Tosh *et al*. [27] have modeled a three-layer game theoretic framework in which the players are organizations, adversaries, and the insurer, where the organization look for the optimal self-defense investment considering sharing cybersecurity information and cyber-insurance, the adversary aims to find the proper attack rate, and the insurer's goal is to find the best coverage level. Khalili *et al*. [26] have investigated the premium discrimination model based on pre-screening to improve the insurer's profits and circumvent the moral hazard problem. Moreover, the benefits of pre-screening in increasing the profit for the insurer and improving the network security have been studied in [19]. A differentiated pricing framework for security vendors has been proposed in [20] to improve the cyber-insurance market. In [25], the authors have studied the design of an incentive-compatible and attack-aware insurance policy by formulating a bi-level game framework to model the interaction of users, attackers, and insurers. The effect of risk interdependency on insurer's utility has been studied in [21], [28]. The result shows that the risk interdependency provides more profit to an insurer.

In contrast to these research studies, in this work, we investigate the benefits of coalitional approaches for insuring a common platform. To this end, we propose several mechanisms where organizations collaboratively participate in the insurance process.

2.3 Cybersecurity Information Sharing

Cybersecurity information sharing is an important parameter to improve the effectiveness of malicious behavior detection. It helps organizations to proactively defend against sophisticated attacks while increasing the accuracy of attack detection. Because of that, several laws and initiatives have been legislated to mandate or encourage the governmental and private organizations to share their cybersecurity information. For instance, in the US, Cybersecurity Information Sharing Act (CISA) [29] has been designed to improve cybersecurity through enhanced sharing of information about cybersecurity threats, in the UK Cybersecurity

Information Sharing Partnership (CiSP) [30] is an initiative for industry and government that has been set up to exchange cyber threat information in real time. Furthermore, Information Sharing and Analysis Centers (ISACs) [31] have been founded to facilitate sharing of cybersecurity information in a particular business. Also, to facilitate cybersecurity information sharing, various protocols and specifications have been developed such as TAXII, STIX, and OpenIOC [32]. On the other hand, game theory has been widely used to model the cybersecurity information sharing in the literature [7]–[9], [33]–[36]. In [33], the authors have investigated the influence of the social planner to motivate players toward cybersecurity information sharing and investment. The cybersecurity investment and sharing behavior in a competitive environment has been studied in [8], [34]. Reference [36] has designed a principal-agent model to study the economics of mandatory security breach reporting to authorities. In our previous work [35], we have applied a coalitional game theory approach to model a fair rewarding and participation-fee in a cybersecurity information sharing platform.

Considering these research studies and leveraging the cyber-insurance, we present mechanisms to push organizations toward sharing behavior in the system by distributing the risks of a common platform.

3 System Model

In this section, we elaborate the system model of a coalitional cyber-insurance framework for a common platform. First, we model the cyber-insurance for a common platform, then we model the cybersecurity information sharing in the coalition, and finally, we discuss the design objectives.

3.1 Cyber-Insurance

Let $\mathcal{O} = \{o_1, ..., o_n\}$ represent the strategic organizations participating in a coalition of cybersecurity information sharing for a common platform. For simplicity and without loss of generality, we let p represent the probability that the attackers $\mathcal{A}$ (irrespective of their type) discover a new vulnerability for the common platform and exploit it. Note that p can be modeled differently based on the common platform's type, however analyzing and studying the modeling of p is outside the scope of this paper.

Each organization o_i decides on the amount of risk to be transferred to an insurer. This decision is based on the organization's risk aversion and insurance-fee. Organizations can be risk-averse, risk-neutral, or risk-seeker. In a setting with multiple options with same expected gain, a risk-averse organization chooses an option with less risk, the risk-seeker chooses an option with the most risk, and the risk-neutral does not have any priority. A utility function mapping wealth into utility $u(w)$ can describe risk attitude where $\frac{\partial u(w)}{\partial w^2} > 0$. For instance, $u(w)$ is concave for a risk-averse organization $\frac{\partial^2 u(w)}{\partial w^2} < 0$. On the other hand, the insurer is a risk-seeker entity accepting risks of another party in return for a premium. In this paper, the insurance covers the cost of exploitation of the new vulnerabilities associated with a common platform.

Let l_i represent the loss of cyber-attack on o_i, the insurance indemnity is $\pi_i = \alpha_i \times l_i$ where $\alpha_i \in [0, 1]$; $\alpha_i = 1$ indicating the full coverage, and $0 < \alpha_i < 1$ representing the partial coverage. Let β_i denote the premium the insured has to pay for the insurance. The insurance is called *actuarially fair* if the net-payoff is zero. In other words, in the actuarially fair insurance, the premium is equal to the expected value of compensation $\bar{\beta}_i = \pi_i \times p$. The risk-averse agent strictly prefers full coverage in the actuarially fair setting [3]. However, in reality, the premium is higher than the actuarially fair $\hat{\beta}_i = \pi_i \times p + \tau$, where, τ represents the administrative cost which is the insurer's profit and cost of safety capital. When the insurance premium is at least actuarially fair, only risk-averse agents insure themselves [3].

3.2 Cybersecurity Information Sharing

After the establishment of a coalition for cybersecurity information sharing, the probability of successful exploitation of a vulnerability decreases once $\mathcal{A}$ exploits a vulnerability over one of the organizations in the coalition. This is because the exploited organization shares the vulnerability information to the other organizations in the coalition and they patch their systems accordingly. We use $\mu(n) \in [0, 1]$ to describe the epidemic model of the expansion of vulnerability exploitation. $\mu(n) = 0$ indicates that the coalition does not have any benefit as the vulnerability information does not get shared before all of the organizations get exploited. As the value of $\mu(n)$ approaches one, the efficiency of the cybersecurity information sharing coalition increases. The value of $\mu(n)$ depends on the nature of the vulnerability, type of attacker, and the agility of cybersecurity information sharing framework.

There is another set of vulnerabilities where $\mu(n)$ approaches zero. For instance, consider a vulnerability where the time gap between the detection of exploitation and patching the system is large enough (for instance *advanced persistent threats*) allowing $\mathcal{A}$ to exploit other organizations as well. As another example assume an equipped $\mathcal{A}$ capable to attack more than one organization at the same time. Thus, $\mu(n)$ can be interpreted as an index of cybersecurity information sharing impact in a coalition of n organizations. It is expected that with the growth of n, the value of $\mu(n)$ increases as well.

Now let us study the model formally. Let $\mathcal{K}, \bar{\mathcal{K}} \subseteq \mathcal{O}$ represent the set of exploited organizations from a new vulnerability and the set of other organizations in the coalition (complement of $\mathcal{K}$), respectively. Having $k = |\mathcal{K}|$ and $\bar{k} = |\bar{\mathcal{K}}|$, we have $\mathcal{K} \cup \bar{\mathcal{K}} = \mathcal{O}, \mathcal{K} \cap \bar{\mathcal{K}} = \emptyset, k + \bar{k} = |\mathcal{O}|$.

Let $q_{i,k}$ denote the probability that $o_i \in \mathcal{K}$, and $\bar{q}_{i,\bar{k}}$ denote the probability that $o_i \in \bar{\mathcal{K}}$. Note that the matrix $\mathbf{Q} = \{q_{i,k}\}$ is modeling the epidemic model of the expansion of vulnerability exploitation. In other words, we use $\mathbf{Q}$ to model the efficiency of the cybersecurity information sharing for the common platform. If organizations efficiently share the vulnerability information then the vulnerability is getting patched and as a result the number of exploited organizations k decreases. On the other hand, if the vulnerability information has not been shared efficiently (e.g. the time gap between sharing the vulnerability information and patching it is large enough allowing attackers to exploit other organizations as well), the number of exploited organizations k increases.

We summarize the notations used in this paper in Table 1.

3.3 Design Objective

The main objective of our insurance policy design is to improve the security state of organizations by motivating organizations to participate in cybersecurity information sharing and invest in security to find new vulnerabilities in a common platform. To this end, there are several challenges that should be addressed in our design as follows:

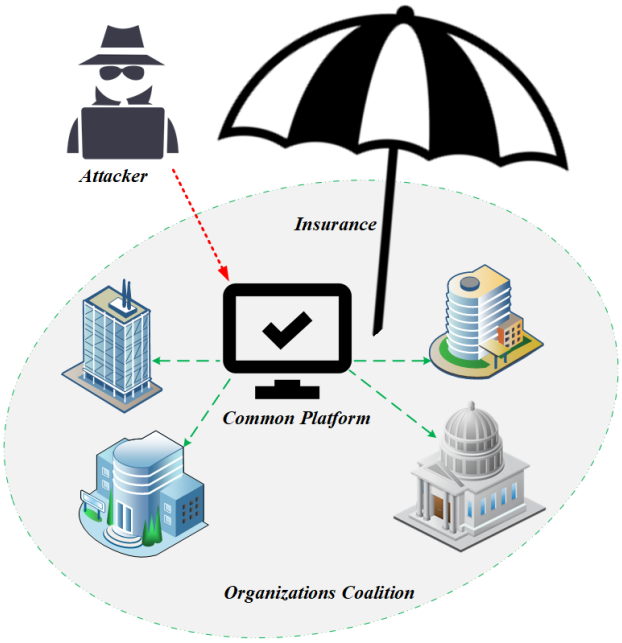

Fig. 1: Organizations Coalition For Cyber-Insurance

- **Adverse selection.** Users with high risk are more likely to take insurance, and an insurer cannot distinguish between insureds before signing the contract. Also, it is not easy to assess the risk of a vulnerability exploitation, and the estimation of the probability of successful attack from insurer and insureds are different. The insurer tends to estimate this value greater than the insureds' estimation. Such information asymmetry causes a discrepancy in the insurance agreement.
- **Moral hazard.** After signing an insurance contract, the insurer might decrease its security investment excessing the chance of a new vulnerability detection by an attacker.
- **Incentive compatibility.** A mechanism is incentive compatible if players can achieve their best outcome by playing based on their true preferences. In interdependent security settings, organizations tend to free-ride such that they do not invest in security or share their cybersecurity information, but getting benefit from the security information shared by the other organizations. We are interested in designing mechanisms where security investment and sharing of cybersecurity information is the organizations' dominant strategy. In this case, the mechanism should be equipped with a rewarding/punishment tool to stipulate organizations for security investment and also sharing cybersecurity information.
- **Fairness.** The costs and benefits should be fairly divided between insurers and insureds based on their efforts and commitments following the insurance policy.

4 Insuring a Common Platform

In this section, we study three models for insuring a common platform. In the first model, organizations act as both insurer and insured to distribute the risk in the coalition. In the second model, the system provides rewards to crowdfund the insurance. Finally, in the third model, we study the outsourcing of a common platform insurance.

4.1 Coalitional Self-Insurance Framework

As organizations use a common platform, they are sharing the same set of vulnerabilities. In order to decrease the cost of cyber-attack over a common platform, we propose a model where organizations distribute the risks among themselves. In our proposed coalitional self-insurance model, every organization o_i in the community commits to an indemnity value c_i. This commitment can be done through payment guarantee contracts. These commitment values will be the source of indemnity when a new vulnerability exploits in the system.

Then, once a new vulnerability of the common platform is exploited, the exploited organizations will be reimbursed based on the organizations' commitments pool.

Having such a model, we have the following benefits:

- Organizations are stipulated to invest in security and share their cybersecurity information in a more efficient way. This is due to the fact that the loss of a vulnerability exploitation for every organization in the coalition is costly for other organizations as well.
- As the exploited organizations need to prove the exploitation of the vulnerability to get reimbursed by the system, they should share the vulnerability information to other organizations in the coalition. Therefore, other organizations are able to patch their systems afterward.
- Organizations share the cost of cyber-attack and transfer the risks to the system without paying the administrative cost of an insurance.

Let $\hat{c}_{i,\bar{k}}$ represent the payment of o_i to community when k organizations are exploited, and let $\hat{\pi}_{i,k}$ represent the indemnity that o_i receives when k organizations are exploited by a new vulnerability of the common platform.

Then, following this model, we can represent the expected utility of an organization o_i in the coalition as

$$\mathbb{E}[u_i] = p(\sum_{k=1}^{n} q_{i,k} \cdot (-l_i + \hat{\pi}_{i,k}) + \bar{q}_{i,n-k} \cdot (-\hat{c}_{i,n-k})) \quad (1)$$

$$s.t. \quad \sum_{k=1}^{n} q_{i,k} + \sum_{k=1}^{n} \bar{q}_{i,k} = 1, \quad \hat{\pi}_{i,n} = 0, \hat{c}_{i,0} = 0$$

Note that in this model, when all of the organizations get exploited, we have $\hat{\pi}_{i,n} = 0, \hat{c}_{i,0} = 0$.

Then the problem is how to calculate the proper value for $\hat{c}_{i,\bar{k}}$ and $\hat{\pi}_{i,k}$ to satisfy the requirements mentioned in section 3.3 in addition to the *ex ante* individual rationality and the budget balanced properties defined as follows:

***Ex ante* individual rationality.** This requires that an agent's expected utility in the framework should be greater than its expected utility outside the framework. *Ex ante* individual rationality attracts agents to participate in the framework. Also, we define the *ex ante* weak individual rationality when the expected utility of an organization does not change whether it is in the framework or not.

Budget balanced. As the resource of indemnity is the commitment values, we need to satisfy the budget balanced property as follows

$$\sum_{i \in \mathcal{K}} \hat{\pi}_{i,k} = \sum_{i \in \bar{\mathcal{K}}} \hat{c}_{i,\bar{k}}$$

Specifying our requirements, now let's study the design of mechanisms which satisfies these properties. A mechanism can be specified by a game $g : \mathcal{M} \to \mathcal{U}$ where $\mathcal{M} = \{m_1, ..., m_n\}$ is a set of input messages and $\mathcal{U} = \{u_1, ..., u_n\}$ is the output of the mechanism. A player chooses its message m_i to increase its utility u_i. In what follows, we present the first mechanism to fulfill the system requirements.

Mechanism 1. Organizations submit their proposed values $\bar{\boldsymbol{\psi}} = \{\psi_1, ..., \psi_n\}$ for the commitment. Let $\hat{\psi} = \min \bar{\boldsymbol{\psi}}$, then the commitment and the indemnity of each organization are calculated as

$$\hat{c}_{i,\bar{k}} = \hat{\psi}$$
$$\hat{\pi}_{i,k} = \frac{\bar{k} \cdot \hat{\psi}}{k}$$

(Note that, here $\mathcal{M} = \bar{\boldsymbol{\psi}}$ and u_i obtains from (1)).

Proposition 1. *The budget balanced property is held in mechanism 1.*

Proof. We need to show that the total of the committed values is equal to the total indemnity value, which is given to the exploited organizations.

$$\sum_{o_i \in \bar{\mathcal{K}}} \hat{c}_{i,\bar{k}} = \sum_{o_i \in \bar{\mathcal{K}}} \hat{\psi} = \bar{k} \cdot \hat{\psi}$$
$$\sum_{o_i \in \mathcal{K}} \hat{\pi}_{i,k} = \sum_{o_i \in \mathcal{K}} \frac{\bar{k} \cdot \hat{\psi}}{k} = \bar{k} \cdot \hat{\psi}$$

□

Proposition 2. *Assume the number of exploited organizations in the coalition is identically distributed $k \sim U[0, n]$, and the probability of exploitation/not-exploitation of an organization is a fair coin, then mechanism 1 satisfies the ex ante individual rationality and the expected benefit for each organization is:*

$$\mathbb{E}[u_i] - \mathbb{E}[u_i^0] = p(\frac{\hat{\psi}}{2n}(\frac{(n-2)}{2} + ... + \frac{1}{n-1})) \qquad (2)$$

Proof. For *ex ante* individual rationality, we need to show that, the expected utility of an organization in the coalition is higher than the expected utility of an organization outside of the coalition $\mathbb{E}[u_i] \geq \mathbb{E}[u_i^0]$. The expected utility of o_i outside of coalition can be calculated as

$$\mathbb{E}[u_i^0] = p(\sum_{k=1}^{n} q_{i,k} \cdot (-l))$$

In the case of applying the model, the expected utility of o_i is

$$\mathbb{E}[u_i] = p(q_{i,1} \cdot (-l_i + \frac{(n-1) \cdot \hat{\psi}}{1}) + \bar{q}_{i,n-1} \cdot (-\hat{\psi}) +$$
$$q_{i,2} \cdot (-l_i + \frac{(n-2) \cdot \hat{\psi}}{2}) + \bar{q}_{i,n-2} \cdot (-\hat{\psi}) + ... +$$
$$q_{i,n-1} \cdot (-l_i + \frac{\hat{\psi}}{n-1}) + \bar{q}_{i,1} \cdot (-\hat{\psi}) + q_{i,n} \cdot (-l_i))$$

As the number of exploited organizations in the coalition is identically distributed and the probability of exploitation/not-exploitation of an organization is a fair coin, we have $\sum_{k=1}^{n} q_{i,k} = \sum_{k=1}^{n} \bar{q}_{i,k} = \frac{1}{2}$ and $q_{i,1} = q_{i,2} = ... = q_{i,n} = \bar{q}_{i,1} = \bar{q}_{i,2} = ... = \bar{q}_{i,n} = \frac{1}{2n}$, therefore we can write the o_i's expected utility as

$$\mathbb{E}[u_i] = p(\sum_{k=1}^{n} q_{i,k} \cdot (-l)) +$$
$$p(\frac{\hat{\psi}}{2n}((n-1) + \frac{(n-2)}{2} + ... + \frac{1}{n-1} - (n-1)))$$

As $n \geq 2$, we have $\mathbb{E}[u_i] \geq \mathbb{E}[u_i^0]$. □

When the number of exploited organizations in the coalition is identically distributed $\mathcal{K} \sim U[0, n]$, by extending Proposition 2, we have the following observations:

- When the probability of exploitation is higher than the probability of not-exploitation ($q_{i,x} > \bar{q}_{i,y}, \forall i, x, y$), then mechanism 1 is *ex ante* individually rational. In this case, with the increase in the number of organizations in the coaltion, the expected utility is also increasing.
- When the probability of exploitation is less than the probability of not-exploitation ($q_{i,x} < \bar{q}_{i,y}, \forall i, x, y$), then mechanism 1 is *ex ante* individually rational if the following inequality holds:
$$(\frac{\frac{(n-2)}{2} + \frac{(n-3)}{3} ... + \frac{1}{n-1}}{(n-1)}) \geq (\bar{q}_{i,y} - q_{i,x})$$
In this case, with the increase in the number of organizations in the coalition, the expected utility is decreasing.
- In an *ex ante* individually rational setting, organizations' utilities increase with the increase in $\hat{\psi}$. Also, with the increase in the number of organizations in the coalition, the expected utility is increasing as well.

Proposition 3. *When the probability of exploitation/not-exploitation of an organization is a fair coin and $n > 2$, the mechanism is ex ante individual rational if $q_{i,k} = 0, \forall k > 1$.*

Proof. When the probability of exploitation/not-exploitation of an organization is a fair coin, we have $q_{i,k} = \bar{q}_{i,k} = \binom{n}{k} \cdot (\frac{1}{2})^n$, thus the expected benefit of the mechanism is

$$\mathbb{E}[u_i] - \mathbb{E}[u_i^0] = p(\hat{\psi} \cdot (\frac{1}{2})^n \cdot (\binom{n}{1}((n-1)-1) +$$
$$\binom{n}{2}(\frac{n-2}{2} - 1) + ... + \binom{n}{n-1}(\frac{1}{n-1} - 1)))$$

The above equation is negative for $n > 2$. However, when $k = 1$ the expected benefit is

$$\mathbb{E}[u_i] - \mathbb{E}[u_i^0] = p(\hat{\psi} \cdot (\frac{1}{2})^n \cdot (\binom{n}{1}((n-1)-1)))$$

Which is always positive. □

In order to satisfy the *ex ante* individual rationality when the probability of exploitation/not-exploitation of an organization is a fair coin, we can modify mechanism 1 such that only the first organization which reports the exploitation will be reimbursed. This also accelerates the flow of cybersecurity information sharing, and organizations are stipulated to investigate the security breaches in the early stages to report damages. By applying this method and following proposition 3, we can see that when $q_{i,1} \geq \bar{q}_{i,1}$ the mechanism is *ex ante* individual rational, and when $q_{i,1} < \bar{q}_{i,1}$, the mechanism is *ex ante* individual rational

if $(q_{i,1}(n-1) - \bar{q}_{i,1}) \geq 0$. In other words, this observation indicates that as the probability of not-exploitation is increasing, the organizations' utilities are decreasing in mechanism 1.

Improvement

Note that in mechanism 1, as all of the organizations in the coalition should be able to afford $c_i = \hat{\psi}$, the value of $\hat{\psi}$ has been set to the least amount between all of the proposed values from the organizations. However, this limits the benefits organizations can receive from the coalition especially when the variance of the proposed values $\bar{\boldsymbol{\psi}}$ is high. For instance, assume a coalition of three organizations, where a small organization o_1 would set $\psi_1 = \$1000$, while the other two big organizations o_2 and o_3 would set $\psi_2 = \psi_3 = \$100,000$, in this case, $\hat{\psi} = \$1000$ will be selected. However, the coalition of two big companies will bring more values for them since in that case $\hat{\psi}$ will be $\$100,000$. On the other hand, a malicious organization o_i would bid a small value for ψ_i to decrease the performance of other organizations in the coalition. To solve this problem, we present the extension of mechanism 1 to make a set of coalitions as follows.

Mechanism 1 extension. Following mechanism 1, after making the first coalition, the organization with the least proposed value is removed from the coalition and the process is repeated by setting the new proposed values as $\psi_i = \psi_i - \hat{\psi}$. The iteration continues until two organizations remain in the coalition.

We explain the mechanism 1 extension with an example. Consider the previous example with three organizations and proposed values as $\bar{\boldsymbol{\psi}} = \{1000, 100000, 100000\}$. In this case, in the first iteration, $\hat{\psi}$ will be set to 1000. After the first iteration, o_1 will be removed, and the new coalition is $\{o_2, o_3\}$, with $\bar{\boldsymbol{\psi}} = \{99000, 99000\}$, thus the new $\hat{\psi}$ will be set to $99,000$. Assume that an attacker exploits a new vulnerability of a common platform over o_1, o_2. Then, o_3 pays $\$1000$ for the first coalition of the three organizations, and o_1, o_2 each receives $\$500$ as indemnity. On the other hand, o_3 pays $\$99,000$ to o_2 for the second coalition.

Claim 1. Mechanism 1 alleviates the moral hazard and adverse selection problems, and it is incentive compatible.

It is easy to see that, as in mechanism 1, the organizations act as both insurer and insured, the moral hazard and adverse selection requirements are alleviated. On the other hand, since growing the number of exploited organizations decrease all of the organizations' utilities, then organizations are stipulated to invest in security and share their vulnerability information in the system which makes the system incentive compatible.

■

Fairness Issue

When the probability of exploitation of each organization is equal, as the exploited organizations receive the same amount while other organizations are paying the same amount to the system, the fairness property is satisfied in mechanism 1. However, when the probability of exploitation is not equal, mechanism 1 is not fair. As the risk of exploitation of organizations is different, their payment and indemnity should be set accordingly to satisfy the fairness property.

For example, consider that there are two organizations using the same platform, and they have made a coalition. An attacker finds a new vulnerability but as he is resource bounded, it is not possible to attack both organizations at the same time. In addition, the attacker knows that the exploited organization is going to share the vulnerability information with the other organization and the other organization will patch its system afterward. In this case, the attacker chooses an organization with the highest benefit to attack. Hence, we have $q_{1,1} \neq q_{2,1}$. Therefore, if we set the $\hat{c}_{i,\bar{k}}$ and $\hat{\pi}_{i,k}$ following mechanism 1, then the *ex ante* individual rationality and fairness property will not be satisfied. In this case, we can apply the following mechanism.

Mechanism 2. Once the system receives the organizations' proposed values for the commitment $\bar{\boldsymbol{\psi}} = \{\psi_1, ..., \psi_n\}$, the commitment and indemnity for all of the organizations are calculated as

$$\hat{c}_{i,\bar{k}} = \hat{\psi} \cdot q_{i,k}$$
$$\hat{\pi}_{i,k} = \frac{\sum_{i \in \bar{\mathcal{K}}} q_{i,k} \cdot \hat{\psi}}{k}$$

Note that in mechanism 2, the commitment and indemnity values are tuned based on the probability of an attack to meet the fairness property.

Proposition 4. *The mechanism 2 satisfies the budget balanced property.*

Proof. We need to show that the total commitment values are equal to the total reimbursements.

$$\sum_{i \in \bar{\mathcal{K}}} \hat{c}_i = \sum_{i \in \bar{\mathcal{K}}} \hat{\psi} \cdot q_{i,k}$$
$$\sum_{i \in \mathcal{K}} \hat{\pi}_{i,k} = \sum_{i \in \mathcal{K}} \frac{\sum_{j \in \bar{\mathcal{K}}} q_{j,k} \cdot \hat{\psi}}{k} = \sum_{j \in \bar{\mathcal{K}}} \hat{\psi} \cdot q_{j,k}$$

□

Proposition 5. *The mechanism 2 satisfies the ex ante individual rationality property if the following inequality holds*

$$\sum_{j \in \{\textbf{-i}\}} \frac{q_{j,k}}{k} \geq \bar{q}_{i,n-k}, \quad \forall i, k$$

*Where $\{$**-i**$\}$ is the set of organizations in the coalition except o_i.*

Proof. For *ex ante* individual rationality, we need to show that, the expected utility of an organization in the coalition is higher than the expected utility of an organization outside of the coalition $\mathbb{E}[u_i] \geq \mathbb{E}[u_i^0]$. Using the mechanism 2, we can expand the o_i's expected utility as

$$\mathbb{E}[u_i] = p(q_{i,1} \cdot (-l + \frac{\sum_{j \in \{\textbf{-i}\}} q_{j,1} \cdot \hat{\psi}}{1}) + \bar{q}_{i,n-1} \cdot (-\hat{\psi} \cdot q_{i,1})$$
$$+ q_{i,2} \cdot (-l + \frac{\sum_{j \in \{\textbf{-i}\}} q_{j,2} \cdot \hat{\psi}}{2}) + \bar{q}_{i,n-2} \cdot (-\hat{\psi} \cdot q_{i,2})$$
$$+ ... + q_{i,n-1} \cdot (-l + \frac{\sum_{j \in \{\textbf{-i}\}} q_{j,n-1} \cdot \hat{\psi}}{n-1}) + \bar{q}_{i,1} \cdot (-\hat{\psi} \cdot q_{i,n-1}))$$

As $\mathbb{E}[u_i^0] = p(\sum_{k=1}^{n} q_{i,k} \cdot (-l))$, then $\mathbb{E}[u_i]$ can be written as

$$\mathbb{E}[u_i] = \mathbb{E}[u_i^0] +$$
$$p((q_{i,1} \cdot \hat{\psi})(\frac{\sum_{j \in \{\textbf{-i}\}} q_{j,1}}{1} - \bar{q}_{i,n-1}) +$$
$$(q_{i,2} \cdot \hat{\psi})(\frac{\sum_{j \in \{\textbf{-i}\}} q_{j,2}}{2} - \bar{q}_{i,n-2}) +$$
$$... + (q_{i,n-1} \cdot \hat{\psi})(\frac{\sum_{j \in \{\textbf{-i}\}} q_{j,n-1}}{n-1} - \bar{q}_{i,1}))$$

From the above equation, it can be seen that when $\forall i, k$ we have $\sum_{j\in\{\textbf{-i}\}} \frac{q_{j,k}}{k} \geq \bar{q}_{i,n-k}$, then $\mathbb{E}[u_i] \geq \mathbb{E}[u_i^0]$.

□

Mechanism 2 extension. As it can be seen from proposition 5, with the growth of the number of exploited organizations, the system moves toward violating the *ex ante* individual rationality property. Thus, in order to satisfy the *ex ante* individual rationality property, we can set the policy to just reimburse the first $\hat{k}$ organizations which report the damage of exploitation of a new vulnerability. Here, $\hat{k}$ is the maximum number satisfying the $\sum_{j\in\{\textbf{-i}\}} \frac{q_{j,\hat{k}}}{\hat{k}} \geq \bar{q}_{i,n-\hat{k}}, \quad \forall i$. As the function $\sum_{j\in\{\textbf{-i}\}} \frac{q_{j,\hat{k}}}{\hat{k}} - \bar{q}_{i,n-\hat{k}}, \forall i$ is decreasing with increasing of $\hat{k}$, $\hat{k} \leq n$, and n is not large, then $\hat{k}$ can be found by exhaustive search. This approach also accelerates the flow of cybersecurity information sharing, and organizations are stipulated to investigate the security breaches at early stages to report damages. Moreover, the same approach introduced in the mechanism 1 extension can be applied to improve the performance of mechanism 2 by making several coalitions based on the proposed commitment values.

Claim 2. The mechanisms 2 alleviates the moral hazard and adverse selection problems, and it is fair and incentive compatible.

Same as mechanism 1, as the organizations act as both insurer and insured, the moral hazard and adverse selection requirements are alleviated. On the other hand, since the exploitation of an organization decreases all of the organizations' utilities, then organizations are stipulated to invest in security and share their vulnerability information in the system which makes the system incentive compatible. Also, as only the first $\hat{k}$ exploited organizations are reimbursed, organizations tend to invest in monitoring security breaches and report them as early as possible. This empowers the cybersecurity information sharing. Moreover, as the organizations' commitment and reimbursement to the system are based on the probability of their exploitation, the fairness property will be satisfied as well.

■

Flexibility Challenge

Although mechanisms 1 and 2 are beneficial for the organizations, they do not allow organizations to set their indemnity value directly. If a mechanism allows the organizations to choose their own values for indemnity and commitment, then as the system should satisfy the budget balanced property, the organizations who commit to less value achieve more utility. This makes the $c_i = 0$ the best response strategy of the organizations. On the other hand, when the loss value is large, organizations might not be able to cover the cost of loss and as a result, the total commitment value can be far from the required loss coverage. In order to solve this problem, in the next sections, we study the mechanisms to give the flexibility of choosing commitment and indemnity to the organizations. To this end, we apply the premium and reward in the design to satisfy the budget balanced property and motivate organizations to make the commitment.

4.2 Crowdfunding the Coalitional Insurance Framework with Different Level of Indemnity and Commitment

In this section we study a model which is equipped to the premium and reward, to let organizations choose the coverage level and the commitment while satisfying the budget balanced property. Furthermore, this model achieves outsiders participation by providing a reward to them.

As the system should be budget balanced, the total value of the rewards should be equal to the total premium values. Let $\boldsymbol{c} = \{\hat{c}_{i,j}\}, \forall i, j$ and $\boldsymbol{\beta} = \{\beta_i\}, \forall i$. The reward value, o_i receives from the system can be represented as $\mathcal{R}_i(\boldsymbol{c}, \boldsymbol{\beta}) : \mathbb{R}^{+^n} \times \mathbb{R}^{+^n} \to \mathbb{R}^+$. In addition, we have $\frac{\partial \mathcal{R}_i(\boldsymbol{c},\boldsymbol{\beta})}{\partial c_i} > 0$ as the reward value is an increasing function of the commitment value to the system. Then, the o_i's expected utility is

$$\mathbb{E}[u_i] = p(\sum_{k=1}^{n} q_{i,k} \cdot (-l_i + \hat{\pi}_{i,k}) + \bar{q}_{i,n-k} \cdot (-\hat{c}_{i,n-k})) + (1-p) \cdot \mathcal{R}_i(\boldsymbol{c}, \boldsymbol{\beta}) - \beta_i$$
$$s.t. \quad \sum_{k=1}^{n} q_{i,k} + \sum_{k=1}^{n} \bar{q}_{i,\bar{k}} = 1, \hat{\pi}_{i,n} = 0, \hat{c}_{i,0} = 0$$

We set reward as $\mathcal{R}_i(\boldsymbol{c}, \boldsymbol{\beta}) = \frac{\sum_{i=1}^{n} \beta_i}{\sum_{i=1}^{n}\sum_{j=1}^{n} c_{i,j}} \times \sum_{j=1}^{n} c_{i,j}$ to meet the fairness requirement. Because of the reward value, this model motivates the risk-seeker entities out of the coalition to participate in the insurance process as well.

In this model, the reward and premium values are controller variables to stabilize the system. To increase the total commitment value, the system can increase the reward, which causes the increase of premium. In contrast, the system can decrease the premium, by decreasing the reward that causes the decrease of the total commitment value.

It can be seen that in the worst case scenario o_i commits to c_i and does not insure itself, thus it endures the full cost of commitment payment and the loss of attack, and its utility will be $u_i = -l_i - c_i$. Conversely, in the best case scenario, o_i does not insure itself and no organization is getting exploited, thus its utility will be $u_i = \mathcal{R}_i(\boldsymbol{c}, \boldsymbol{\beta})$. The worst case scenario and the best case scenario happen to the risk-seeker organizations, while the risk-averse organizations enroll in the insurance.

Note that in this model as the organizations are charged based on their coverage level, they should be reimbursed in the case of a cyber-attack. However, it is not always possible to satisfy the budget balanced property since as the number of exploited organizations grows, the available budget in the pool decreases. To solve this problem, we present two approaches as follows.

Approach 1. In order to satisfy the budget balanced property and motivate organizations to share their cybersecurity information, the system can set its policy such that only the first organization, which reports the exploitation of a new vulnerability, receives the reimbursement. This mechanism works as follows; At the beginning, organizations submit their desired commitment values $\{c_i\}$ to the system. Then organizations choose their coverage level π_i from $0 \leq \pi_i \leq \sum_{j\in\{\textbf{-i}\}} c_j$. In this case, having the actuarially fair premium, o_i's expected utility is

$$\mathbb{E}[u_i] = p(q_{i,1} \cdot (-l_i + \pi_i) + \bar{q}_{i,n-1} \cdot (-\frac{\pi_{\kappa\in\mathcal{K}}}{\sum_{j\in\bar{\mathcal{K}}} c_j} c_i)) + (1-p) \cdot (\frac{p \cdot \sum_{j=1}^{n} q_{j,1} \cdot \pi_j}{\sum_{j=1}^{n} c_j} \cdot c_i) - (p \cdot q_{i,1} \cdot \pi_i)$$

In this case, organizations are stipulated to investigate the security breaches and accelerate the reporting of such information; this improves the flow of cybersecurity information in the coalition.

Proposition 6. *Approach 1 satisfies the budget balanced property.*

Proof. For the budget balanced property, we need to show that the total commitment received from the organizations is equal to the

indemnity which the exploited organization will be reimbursed, and the total rewards are equal to the total premiums.

$$\sum_{i\in\bar{\mathcal{K}}} \frac{\pi_{\kappa\in\mathcal{K}}}{\sum_{j\in\bar{\mathcal{K}}} c_j} \cdot c_i = \frac{\pi_{\kappa\in\mathcal{K}}}{\sum_{j\in\bar{\mathcal{K}}} c_j} \cdot \sum_{i\in\bar{\mathcal{K}}} c_i = \pi_\kappa$$

And

$$\sum_{i=1}^{n} \mathcal{R}_i(\boldsymbol{c},\boldsymbol{\beta}) = \sum_{i=1}^{n} (\frac{p \cdot \sum_{j=1}^{n} q_{j,1} \cdot \pi_j}{\sum_{j=1}^{n} c_j} \cdot c_i) = \sum_{i=1}^{n} p \cdot q_{i,1} \cdot \pi_i = \sum_{i=1}^{n} \beta_i$$

□

Discussion

This model does not satisfy *ex ante* individual rationality and as a result a risk-neutral organization's best response strategy is to bid $\hat{c}_i = 0, \hat{\pi}_i = 0$. However, the risk-averse organization's best response strategy is to bid $\hat{\pi}_i = l_i, \hat{c}_i = 0$ as the premium is actuarially fair. On the other hand, the risk-seeker entities would set $\hat{\pi}_i = 0, \hat{c}_i > 0$ and selects $\hat{c}_i$ based on its budget and risk function. Thus, this model will be advantageous if and only if we have risk-seeker organizations in the model. In order to achieve this, the platform can allow other entities outside of the coalition to participate in the insurance process as well. In this case, the risk-seeker entities make a commitment with the goal of receiving a reward from the premiums organizations pay to the coalition. This crowd-funding model allows organizations to have more power on the price of cyber-insurance to avoid a monopoly market.

Approach 2. As another approach, the system can reimburse the organizations based on the total exploited organizations and the available budget in the pool. In this case, the available budget will be distributed fairly among the exploited organizations. The system charges organizations based on their expected coverage level. Let us define $\Gamma(\pi_i)$ as follows

$$\Gamma(\pi_i) = \begin{cases} \pi_i & \sum_{j\in\mathcal{K}} \pi_j \leq \sum_{j\in\bar{\mathcal{K}}} c_j \\ \frac{\sum_{j\in\bar{\mathcal{K}}} c_j}{\sum_{j\in\mathcal{K}} \pi_j} \cdot \pi_i & \text{Otherwise} \end{cases}$$

As the organizations should pay their premium based on the expected coverage that they will be reimbursed in the case of exploitation, then assuming that the organizations are exploited with the same probability, the fair premium is

$$\hat{\beta}_i = p(q_{i,1} \cdot (\Gamma(\pi_i)) + q_{i,2} \cdot (\Gamma(\pi_i + \bar{\pi}_{-i})) + q_{i,3} \cdot (\Gamma(\pi_i + 2 \times \bar{\pi}_{-i})) + ... + q_{i,n-1} \cdot (\Gamma(\pi_i + (n-2) \cdot \bar{\pi}_{-i}))$$

Where $\bar{\pi}_{-i}$ represents the average indemnity of the organizations in the coalition excluding o_i. In addition, the commitment value is

$$\hat{c}_i = \begin{cases} c_i & \sum_{j\in\bar{\mathcal{K}}} c_j \leq \sum_{j\in\mathcal{K}} \pi_j \\ \frac{\sum_{j\in\mathcal{K}} \pi_j}{\sum_{j\in\bar{\mathcal{K}}} c_j} \cdot c_i & \text{Otherwise} \end{cases}$$

Proposition 7. *Approach 2 satisfies the budget balanced property.*

Proof. We need to show that the total commitment value is equal to the total reimbursement value. When $\sum_{j\in\bar{\mathcal{K}}} c_j \leq \sum_{j\in\mathcal{K}} \pi_j$ we have

$$\sum_{i\in\bar{\mathcal{K}}} \hat{c}_i = \sum_{i\in\bar{\mathcal{K}}} c_i$$

$$\sum_{i\in\mathcal{K}} \Gamma(\pi_i) = \sum_{i\in\mathcal{K}} \frac{\sum_{j\in\bar{\mathcal{K}}} c_j}{\sum_{j\in\mathcal{K}} \pi_j} \cdot \pi_i = \sum_{j\in\bar{\mathcal{K}}} c_j$$

And when $\sum_{j\in\mathcal{K}} \pi_j \leq \sum_{j\in\bar{\mathcal{K}}} c_j$ we have:

$$\sum_{i\in\bar{\mathcal{K}}} \hat{c}_i = \sum_{i\in\bar{\mathcal{K}}} \frac{\sum_{j\in\mathcal{K}} \pi_j}{\sum_{j\in\bar{\mathcal{K}} c_j}} \cdot c_i = \sum_{j\in\mathcal{K}} \pi_j$$

$$\sum_{i\in\mathcal{K}} \Gamma(\pi_i) = \sum_{i\in\mathcal{K}} \pi_i$$

□

Outsider Participation

As we have discussed earlier, in this model, the risk-seeker entities outside the coalition is also able to invest in the insurance with the goal of receiving a reward. In this case, the premium and reward should be set in such a way to attract outsiders to invest in the system. In other words, the *ex ante* individual rationality property for the outsiders should be satisfied. Therefore, the expected utility of an entity outside of the coalition should be larger than zero $\mathbb{E}[\boldsymbol{u}_{ext}(c_{ext})] > 0$. Let $\tilde{\beta} = ||\boldsymbol{\beta}||_1$ represent the total premium collected from the coalition. Algorithm 1 can be used to achieve this goal. In this algorithm, the premium has been set to satisfy the *ex ante* individual rationality for the external entities. First, the expected indemnity cost and the expected available budget are calculated in lines 1-6. Then, in lines 7 and 12, the algorithm compares the expected indemnity cost and expected available budget to check the corresponding requirement. In case $\tilde{c} \leq \tilde{\pi}$, the following should be held

$$\mathbb{E}[\boldsymbol{u}_{ext}(c_{ext}|\tilde{c} \leq \tilde{\pi})] = p(-c_{ext}) + (1-p)(\frac{\tilde{\beta}}{(\sum_{j=1}^{n} c_j + c_{ext})} \cdot c_{ext}) > 0 \Rightarrow \tilde{\beta} > \frac{p \cdot (\sum_{i=1}^{n} c_i + c_{ext})}{1-p}$$

And in case $\tilde{\pi} < \tilde{c}$ the following requirement should be satisfied

$$\mathbb{E}[\boldsymbol{u}_{out}(c_{ext}|\tilde{\pi} < \tilde{c})] = p(-\frac{\tilde{\pi}}{(\tilde{c} + c_{ext})} \cdot c_{ext}) + (1-p)(\frac{\tilde{\beta}}{\sum_{i=1}^{n} c_i + c_{ext}} \cdot c_{ext}) > 0 \Rightarrow \tilde{\beta} > \frac{p \cdot \tilde{\pi} \cdot (\sum_{i=1}^{n} c_i + c_{ext})}{(1-p) \cdot (\tilde{c} + c_{ext})}$$

If the requirement satisfies, then the algorithm exits, otherwise the premium value increases in lines 9 and 14. Note that this increase can be done based on the fairness definition. For example following the proportional fairness, the organizations will be charged based on their required indemnities. Once the premium has been increased, organizations might lower their coverage level accordingly, thus the algorithm jumps to line 2 to calculate $\tilde{c}$ again.

The complexity of algorithm 1 is $O(2^n.\tilde{\pi})$. This is because the line 4 iterates $(2^n - 1)$ times to calculate the $\tilde{c}$ value, and in the worst case the total requested indemnity decreases to zero in $\tilde{\pi}$ iterations.

Algorithm 1: Tuning premium to acquire external commitment resource

Input : The vector of indemnities $\boldsymbol{\pi}$, The vector of commitments $\boldsymbol{c}$, The matrix of exploitation probability $\boldsymbol{Q}$, The probability that an attacker finds a vulnerability for the common platform p, The desired commitment from an external resource c_{ext}, The total premium $\tilde{\beta}$

Output: The tuned total premium value $\tilde{\beta}$

1 $\tilde{c} \leftarrow 0, \tilde{\pi} \leftarrow 0$
2 $\tilde{\boldsymbol{\pi}} \leftarrow \boldsymbol{\pi}.\boldsymbol{Q}$
3 $\tilde{\pi} \leftarrow ||\tilde{\boldsymbol{\pi}}||_1$
4 **foreach** *possible set of* $\mathcal{K} \in \mathcal{O}$ **do**
5 $\quad \tilde{c} \leftarrow \tilde{c} + \prod_{i \in \mathcal{K}} q_{i,|k|} \cdot \sum_{j \in \bar{\mathcal{K}}} c_j$
6 **end**
7 **if** $\tilde{c} \leq \tilde{\pi}$ **then**
8 $\quad$ **if** $\tilde{\beta} < \frac{p \cdot (\sum_{i=1}^{n} c_i + c_{ext})}{1-p}$ **then**
9 $\quad\quad$ Increase $\tilde{\beta}$, update $\boldsymbol{\pi}$, and **Goto** line 2
10 $\quad$ **end**
11 **end**
12 **if** $\tilde{\pi} < \tilde{c}$ **then**
13 $\quad$ **if** $\tilde{\beta} < \frac{p \cdot \tilde{\pi} \cdot (\sum_{i=1}^{n} c_i + c_{ext})}{(1-p) \cdot (\tilde{c} + c_{ext})}$ **then**
14 $\quad\quad$ Increase $\tilde{\beta}$, update $\boldsymbol{\pi}$, and **Goto** line 2
15 $\quad$ **end**
16 **end**
17 return $\tilde{\beta}$

Proposition 8. *In the case of $\tilde{c} \leq \tilde{\pi}$, outsider's best response strategy is to commit c^*_{ext} as*

$$c^*_{ext} = \sqrt{\frac{(1-p).\tilde{\beta}.\sum_{i=1}^{n} c_i}{p}} - \sum_{i=1}^{n} c_i$$

Proof. As the second derivative of $\mathbb{E}[\boldsymbol{u}_{out}(c_{ext}|\tilde{c} \leq \tilde{\pi})]$ is negative, thus we calculate the first order condition as

$$\frac{\partial \mathbb{E}[\boldsymbol{u}_{out}(c_{ext}|\tilde{c} \leq \tilde{\pi})]}{\partial c_{ext}} = 0$$

$$-p + (1-p)\left(\frac{\tilde{\beta} \cdot \sum_{j=1}^{n} c_j}{((\sum_{j=1}^{n} c_j + c^*_{ext}))^2}\right) = 0$$

$$c^*_{ext} = \sqrt{\frac{(1-p).\tilde{\beta}.\sum_{i=1}^{n} c_i}{p}} - \sum_{i=1}^{n} c_i$$

□

On the other hand, in the case of $\tilde{\pi} < \tilde{c}$ as the second derivative of the outsider's expected utility is positive, it can be seen that the increase of commitment value, increases the expected utility.

4.3 Outsourcing the insurance of a common platform

Although the crowdfunding is beneficial, outsiders might not participate in the insurance process when it cannot estimate the p value. This incapability of estimation might be because of the inaccessibility of a common platform (e.g. hardware) or the lack of expertise. In this case, we study a model of outsourcing the insurance of a common platform to cover the demanded coverage level. In this model, the organizations insure the cost of exploitation of the common platform's vulnerabilities. In the case of exploitation of the vulnerabilities related to the common platform, the insurer reimburses the organizations that have been damaged. The benefits of this model are as follows

- The insurer has a better estimation of the probability of the exploitation p. Since in the traditional cyber-insurance model it is not easy to estimate p as this parameter usually depends on multiple systems working together. On the other hand, there are some limitations to the security evaluation of the entire system. While in this model, the coverage is limited to only the common platform. This comforts the evaluation process and as a result, the adverse selection problem will be addressed partially.
- Monitoring the current security state is easier for the insurer, as the attack vectors are limited to the common platform. This alleviates the moral hazard problem.
- Organizations collaboratively insure a common platform taking advantage of sharing the price of the administrative cost. In contrast, having an incentive compatible mechanism, the insurer profits as the organizations invest more on their security and share their cybersecurity information and as a result, fewer organizations will be exploited and the cost of indemnity would decrease.

Let $\pi_{\mathcal{K}}$ represent the indemnity that the insurer should pay to the coalition considering the set of exploited organizations $\mathcal{K}$. Then, the total premium that the coalition should pay $\hat{\beta}_{\mathcal{O}}$ is

$$\hat{\beta}_{\mathcal{O}} = p(\sum_{i=1}^{n}\sum_{j=1}^{n} q_{i,j} \cdot \pi_i) + \tau$$

And the expected utility of the coalition is

$$\mathbb{E}[u_{\mathcal{O}}] = p(-\sum_{i \in \mathcal{K}} l_i + \pi_{\mathcal{K}}) - \hat{\beta}_{\mathcal{O}}$$

Then to satisfy the fairness property, o_i's premium can be calculated as

$$\hat{\beta}_i = p(\sum_{j=1}^{n} q_{i,j} \cdot \pi_i) + (\sum_{j=1}^{n} q_{i,j} \cdot \tau)$$

Note that, this model is beneficial for the organizations as the administrative cost of the insurer is divided between them. However, as the organizations have outsourced the risk of exploitation, they might decrease their investment in the security of the common platform and they are not motivated to share their cybersecurity information. In order to satisfy the incentive compatibility, the following approaches can be applied.

Approach 1. The insurer does not provide the full coverage. In this case, as the organizations also endure the cost of exploitation, they would invest in the security of the common platform. However, in this case, the incentive compatibility problem is still existing as organizations are not motivated to share their cybersecurity information.

Approach 2. In order to stipulate organizations and free-market security testers to invest in the security of the common platform to find a new vulnerability, the system can provide a bug bounty rewarding system [37]–[39]. In this case, the system pays the vulnerability finder. However, it is important to set a reward value properly, since if the value is small, then there is no motivation for investment in finding a new vulnerability. Worse than that, a free market tester who finds a new vulnerability might sell the vulnerability information on the black market. On the other hand, if the value is high, the organizations and insurance

company might lose. The value of a vulnerability for the coalition of organizations v_c is

$$v_c = \sum_{i=1}^{n}\sum_{j=1}^{n} q_{i,j}(l_i - \pi_i)$$

On the other hand, the value of the vulnerability for the insurer v_I is

$$v_I = \sum_{i=1}^{n}\sum_{j=1}^{n} q_{i,j}(\pi_i)$$

Thus, the total benefit of accessing the vulnerability information to patch the system is $\mathcal{V} = v_c + v_I = \sum_{i=1}^{n}\sum_{j=1}^{n} q_{i,j} \cdot l_i$ which is equal to the case of no insurance being applied. As studied in [35], the fair payment to the vulnerability finder is half of the benefit of the information beneficiaries.

Proposition 9. *Assume there is a black market value v_b for the new vulnerability and this value is an independent draw from a uniform distribution with support $[0, N]$, then the best response strategy of the system is to offer $\frac{\mathcal{V}}{2}$ to the vulnerability finder.*

Proof. Let θ represent the offer to the vulnerability finder. The expected payoff of the system is

$$\begin{aligned}\mathbb{E}[u_s] &= Pr(v_b < \theta) \cdot (\mathcal{V} - \theta) \\ &= (\frac{\theta}{N}) \cdot (\mathcal{V} - \theta)\end{aligned}$$

The first order condition is

$$\frac{\partial((\frac{\theta}{N}) \cdot (\mathcal{V} - \theta))}{\partial\theta} = 0$$
$$\frac{\mathcal{V} - \theta^*}{N} - \frac{\theta^*}{N} = 0$$
$$\theta^* = \frac{1}{2} \cdot \mathcal{V}$$

As the second derivative of the expected gain is negative, θ^* provides the maximum expected gain. □

Proposition 9 shows that, when the market value is not biased, the fair payment and the best response strategy are equal.

Approach 3. In order to motivate organizations to share their cybersecurity information and decrease the probability of exploitation of a large number of organizations from the same vulnerability, the insurer sets one part of the indemnity as the reward value. In this case, there is a fixed amount that is given to the exploited organizations, if the number of exploited organizations is small, the share of reward is large and as the number of organizations grows, this share shrinks. In this way, as with the growth of the exploited organizations the reward value decreases, the organizations tend to share their data in the coalition to receive a larger share of the reward. Let R represent the reward value, then the premiums of the coalition and each organization can be calculated as follows

$$\hat{\beta}_{\mathcal{O}} = p((\sum_{i=1}^{n}\sum_{j=1}^{n} q_{i,j} \cdot \pi_i) + R) + \tau$$

$$\hat{\beta}_i = p(\sum_{j=1}^{n} q_{i,j} \cdot (\pi_i + R)) + (\sum_{j=1}^{n} q_{i,j} \cdot \tau)$$

And the expected utilities of the coalition and each organization are

$$\mathbb{E}[u_{\mathcal{O}}] = p(\sum_{i\in\mathcal{K}} -l_i + \pi_{\mathcal{K}} + R) - \hat{\beta}_{\mathcal{O}}$$

$$\mathbb{E}[u_i] = p(\sum_{j=1}^{n} q_{i,j} \cdot (-l_i + \pi_i + \frac{R}{j})) - \hat{\beta}_i$$

It is easy to see that the above model is budget balanced and incentive compatible to motivate organizations for security investment and sharing behavior.

The combination of the three approaches mentioned above can be used to achieve the best result.

5 Numerical Analysis

In this section, we analyze the expected utility of the proposed models. In the first case study, we consider a set of organizations using a common platform. For simplicity, we assume the number of exploited organizations in the coalition is identically distributed $k \sim U[0, n]$, and the probability of exploitation/not-exploitation of an organization is a fair coin. In order to check the benefit of the coalitional self-insurance framework, we calculate the expected benefit of applying this model. Then, applying the mechanism 1, the profit of an organization in the coalition is $p(\frac{\hat{\psi}}{2n}(\frac{(n-2)}{2} + ... + \frac{1}{n-1}))$ as discussed in proposition 2. Figure 2 depicts the expected benefits of an organization in the coalition when p, $\hat{\psi}$, and n vary. In figures 2 (a) and (b), we have set $p = 0.1$.

As it can be seen with the increase of n (figure 2. (a)), $\hat{\psi}$ (figure 2. (b)), and p (figure 2. (c)), an organization's expected benefit increases with increasing rates. This implies that when the probability of an attack to organizations over the common platform is not biased, organizations' expected benefit is increasing with the growth of the probability of finding a vulnerability by an attacker, the organizations' commitment value, and the number of organizations in the coalition.

In the next case study, we consider a set of risk-averse organizations that aim to cover a specific amount of the indemnity in the case of a cyber-attack. Note that although mechanism 1 or 2 can be applied, as organizations are resource-bounded, they might not be able to commit to large values to cover all of the requested indemnities. For example, consider that a loss of an attack for an organization is $\$1,000,000$ yet the expected coverage level applying mechanism 1 or 2 is $\$10,000$. Thus, in this case, organizations outsource the insurance. The benefit of applying the crowdfunding is that organizations can achieve a cheaper premium for their insurance service by saving the insurance administrative cost. Furthermore, this helps to change a monopolistic insurance market into a competitive market. To analyze the crowdfunding model, we check how the outsiders' commitment value changes with the variation of other parameters. As in this model, the expected coverage level is higher than the expected commitment coverage of organizations in the coalition, we study the case of $\tilde{c} \geq \tilde{\pi}$. In this case, following proposition 8, the outsider chooses $c^*_{ext} = \sqrt{\frac{(1-p).\tilde{\beta}.\sum_{i=1}^{n} c_i}{p}} - \sum_{i=1}^{n} c_i$ to maximize its benefit. Figure 3 depicts an outsider's best response commitment strategy, when the total internal commitment $\sum_{i=1}^{n} c_i$, the probability of finding a new vulnerability p, and the total premium value $\tilde{\beta}$ vary. As it can be seen, with the growth of p and $\sum_{i=1}^{n} c_i$, the outsider commitment decreases with an increasing rate; and with the increase of $\tilde{\beta}$, the outsider commitment increases with a decreasing rate.

Finally, consider the case of outsourcing the insurance of a common platform to an insurer. We follow the model introduced in section 4.3 to collaboratively outsource a common platform to an insurer. In this case, the risk-averse organizations register for the

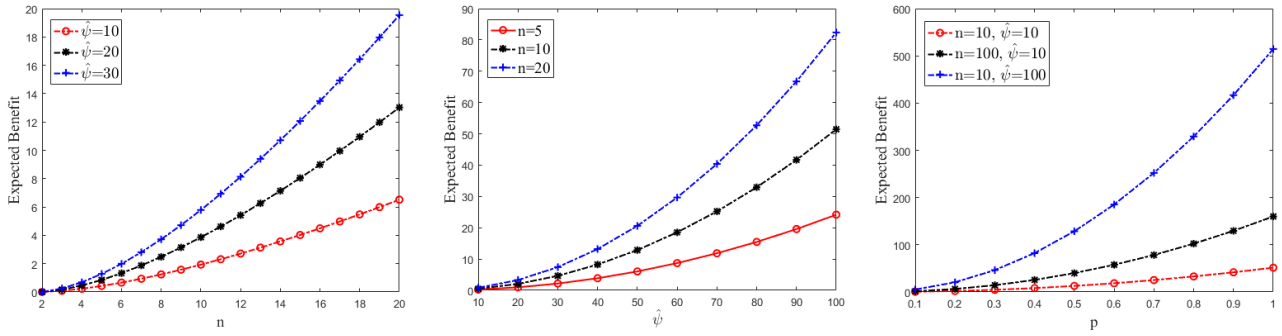

Fig. 2: The changes of expected benefit when p, $\hat{\psi}$, and n vary

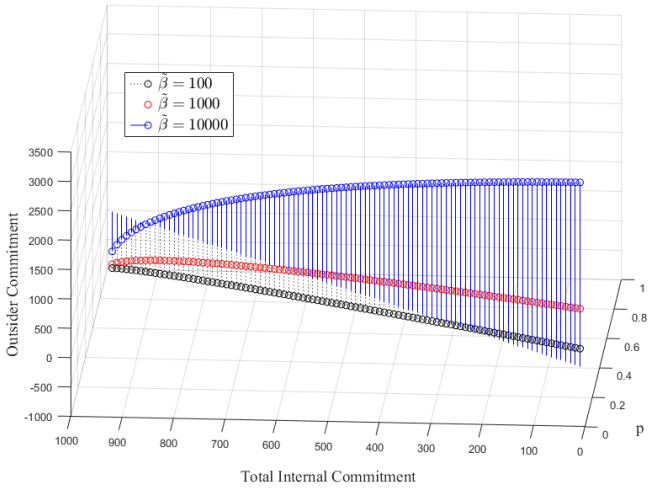

Fig. 3: Outsider commitment value when $\sum_{i=1}^{n} c_i$, p, and $\tilde{\beta}$ vary

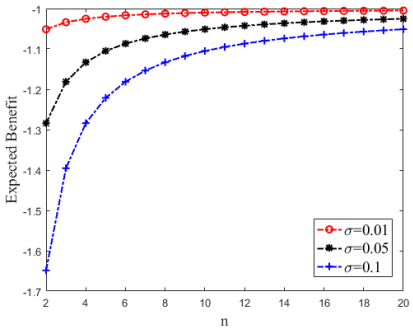

Fig. 4: The expected benefit of a risk-averse organization by cooperatively outsourcing the insurance of a common platform

insurance. We apply Constant Absolute Risk Aversion (CARA) to model the organizations' risk aversion [3], [4]. CARA is one of the most well-known candidate functions to model the utility function considering the risk aversion level. This function maps wealth to utility by $u(w) = -\exp(-\sigma \cdot w)$, where σ indicates the degree of risk aversion. The expected benefit is calculated based on the discount of the administrative cost and also the decrease of exploitation probability by assuming that the organizations in the coalition share the probability of attack between themselves. Figure 4 depicts how the risk-averse organizations benefit from such a model when the number of organizations in the coalition vary. We have set the $\mathbb{E}[u_i^0] = -10$ and we calculated the expected benefit for organizations with different level of risk aversion $\sigma = 0.01, \sigma = 0.05$, and $\sigma = 0.1$. As it can be seen by increasing the number of organizations in the coalition, the organizations' utilities are increasing.

Note that although in this section we have discussed the direct benefits of applying the model, as discussed in the paper, the main advantages of the proposed models are their indirect profits which are the alleviation of the moral hazard, adverse selection, and motivating organizations toward the social welfare by investing in cybersecurity and sharing cybersecurity information.

6 Conclusion

Although cyber-insurance allows organizations to transfer their risk to another party, it has not been deployed as expected. This is mainly because of the insurance policy limitation and its high price. In addition, Moral Hazard and Adverse Selection are two big challenges that make such a process difficult. On the other hand, when the organizations are using a common platform, they are susceptible to a same set of vulnerabilities. Thus, their security is interdependent and their security investment to find a new vulnerability over the common platform causes positive externality. Leveraging cyber-insurance and risk interdependency for a common platform, we have presented three models for insuring a common platform to alleviate Moral Hazard, Adverse Selection, and Free-Riding problems. In the first model, organizations act as both insurer and insured to distribute the risk in the coalition. In the second model, the system provides rewards to crowdfund the insurance. Finally, in the third model, we have studied the outsourcing of a common platform insurance. We presented mechanisms to motivate organizations for security investment and cybersecurity information sharing while cooperatively transferring risks.

References

[1] "Insurance 2020 and beyond: Reaping the dividends of cyber resilience." https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

[2] B. Johnson, R. Böhme, and J. Grossklags, "Security games with market insurance," in *International Conference on Decision and Game Theory for Security*, pp. 117–130, Springer, 2011.

[3] R. Böhme, G. Schwartz, *et al.*, "Modeling cyber-insurance: Towards a unifying framework.," in *WEIS*, 2010.

TABLE 1: Notations used in this paper

Notation	Description
p	The probability that an attacker finds a new vulnerability of the common platform
n	The number of the organizations in the coalition
l_i	o_i's loss from a cyber-attack over the common platform
$\mathcal{K}$	The set of exploited organizations in the coalition
$\bar{\mathcal{K}}$	The set of organizations in the coalition which have not been exploited
$q_{i,k}$	The probability that $o_i \in \mathcal{K}$
$\bar{q}_{i,\bar{k}}$	The probability that $o_i \in \bar{\mathcal{K}}$
π_i	The insurance indemnity to o_i
β_i	The insurance premium for o_i
$\bar{\beta}_i$	The actuarially fair premium
c_i	The o_i commitment for the indemnity
$\hat{c}_{i,\bar{k}}$	The payment of o_i to community when k organizations exploited
$\hat{\pi}_{i,b}$	The indemnity that o_i receives when k organizations exploited
$\tilde{c}$	The expected available budget for reimbursement from the coalition
$\tilde{\pi}$	The expected indemnity
$\{\textbf{-i}\}$	The set of organizations in the coalition except o_i
c_{ext}	The outsider commitment to the coalition
τ	Insurer administrative cost
ψ_i	o_i's bid for the commitment
$\hat{\psi}$	Minimum of the commitment bids submitted by the organizations.
$\boldsymbol{c}$	The vector of the organizations' commitments.
$\boldsymbol{\beta}$	The vector of the organizations' premiums.
$\tilde{\beta}$	The total premium collected from the coalition
$\mathcal{R}_i(\boldsymbol{c}, \boldsymbol{\beta})$	o_i's reward for its commitment.
σ	The degree of risk aversion
v_c	The value of vulnerability information for the coalition
v_I	The value of vulnerability information for the insurer
v_b	The black market value of the vulnerability information
$\mathcal{V}$	The sum of value of the vulnerability information for the coalition and insurer
θ	The system's offer to the vulnerability finder

[4] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey," *Computer Science Review*, vol. 24, pp. 35–61, 2017.

[5] "The heartbleed bug." http://www.heartbleed.com.

[6] "Half a million widely trusted websites vulnerable to heartbleed bug." https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html.

[7] 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.

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

[9] I. Vakilinia, D. K. Tosh, and S. Sengupta, "3-way game model for privacy-preserving cybersecurity information exchange framework," in *Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE*, pp. 829–834, IEEE, 2017.

[10] A. Laszka, M. Felegyhazi, and L. Buttyan, "A survey of interdependent information security games," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, p. 23, 2015.

[11] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, p. 25, 2013.

[12] H. Varian, "System reliability and free riding," in *Economics of information security*, pp. 1–15, Springer, 2004.

[13] L. Jiang, V. Anantharam, and J. Walrand, "How bad are selfish investments in network security?," *IEEE/ACM Transactions on Networking*, vol. 19, no. 2, pp. 549–560, 2011.

[14] L. Xiao, Y. Chen, W. S. Lin, and K. R. Liu, "Indirect reciprocity security game for large-scale wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1368–1380, 2012.

[15] P. Naghizadeh and M. Liu, "Exit equilibrium: Towards understanding voluntary participation in security games," in *Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on*, pp. 1–9, IEEE, 2016.

[16] R. Böhme, "Security audits revisited," in *International Conference on Financial Cryptography and Data Security*, pp. 129–147, Springer, 2012.

[17] F. Farhadi, H. Tavafoghi, D. Teneketzis, and S. J. Golestani, "An efficient dynamic allocation mechanism for security in networks of interdependent strategic agents,"

[18] S. Gritzalis, A. N. Yannacopoulos, C. Lambrinoudakis, P. Hatzopoulos, and S. K. Katsikas, "A probabilistic model for optimal insurance contracts against security risks and privacy violation in it outsourcing environments," *International Journal of Information Security*, vol. 6, no. 4, pp. 197–211, 2007.

[19] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies: The role of pre-screening and security interdependence," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2226–2239, 2018.

[20] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Security pricing as enabler of cyber-insurance a first look at differentiated pricing markets," *IEEE Transactions on Dependable and Secure Computing*, 2017.

[21] M. M. Khalili, P. Naghizadeh, and M. Liu, "Embracing risk dependency in designing cyber-insurance contracts," in *Communication, Control, and Computing (Allerton), 2017 55th Annual Allerton Conference on*, pp. 926–933, IEEE, 2017.

[22] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? a market analysis," in *INFOCOM, 2014 Proceedings IEEE*, pp. 235–243, IEEE, 2014.

[23] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies: Mitigating moral hazard through security pre-screening," in *International Conference on Game Theory for Networks*, pp. 63–73, Springer, 2017.

[24] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand, "Competitive cyber-insurance and internet security," in *Economics of information security and privacy*, pp. 229–247, Springer, 2010.

[25] R. Zhang, Q. Zhu, and Y. Hayel, "A bi-level game approach to attack-aware cyber insurance of computer networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 779–794, 2017.

[26] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies in the presence of security interdependence," in *Proceedings of the 12th workshop on the Economics of Networks, Systems and Computation*, p. 7, ACM, 2017.

[27] D. K. Tosh, I. Vakilinia, S. Shetty, S. Sengupta, C. A. Kamhoua, L. Njilla, and K. Kwiat, "Three layer game theoretic decision framework for cyber-investment and cyber-insurance," in *International Conference on Decision and Game Theory for Security*, pp. 519–532, Springer, 2017.

[28] M. M. Khalili, M. Liu, and S. Romanosky, "Embracing and controlling risk dependency in cyber-insurance policy underwriting,"

[29] https://www.congress.gov/bill/114th-congress/senate-bill/754.

[30] "Cyber-security information sharing partnership (cisp)." https://www.ncsc.gov.uk/cisp.

[31] "Information sharing and analysis centers (isac)." https://www.nationalisacs.org/.

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

[33] 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.

[34] E. Gal-Or and A. Ghose, "The economic incentives for sharing security information," *Information Systems Research*, vol. 16, no. 2, pp. 186–208, 2005.

[35] I. Vakilinia and S. Sengupta, "A coalitional game theory approach for cybersecurity information sharing," in *Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE*, pp. 237–242, IEEE, 2017.

[36] S. Laube and R. Böhme, "The economics of mandatory security breach reporting to authorities," *Journal of Cybersecurity*, vol. 2, no. 1, pp. 29–41, 2016.

[37] "Google vulnerability reward program (vrp)." https://www.google.com/about/appsecurity/reward-program/.

[38] "Facebook whitehat." https://www.facebook.com/whitehat.

[39] "Mozilla bug bounty program." https://www.mozilla.org/en-US/security/bug-bounty/.