Embracing and Controlling Risk Dependency in Cyber-insurance Policy Underwriting

Mohammad Mahdi Khalili[1], Mingyan Liu[1], and Sasha Romanosky[2]

[1]University of Michigan, Ann Arbor MI, USA
[2]RAND Corporation, Arlington VA, USA

Abstract

This paper highlights how cyber risk dependencies can be taken into consideration when underwriting cyber-insurance policies. This is done within the context of a base rate insurance policy framework, which is widely used in practice. Specifically, we show that there is an opportunity for an underwriter to better control the risk dependency and the risk spill-over, ultimately resulting in lower overall cyber risks across its portfolio. To do so, we consider a Service Provider (SP) and its customers as the interdependent insurer's customers: a data breach suffered by the SP can cause business interruption to its customers. In underwriting both the SP and its customers, we show that the insurer can increase its profit by incentivizing the SP (through a discount on its premium) to invest more in security, thereby decreasing the chance of business interruption to the customers and increasing social welfare. For comparison, we also consider a scenario where the insurer underwrites only the SP's customers (but not the SP), and receives compensation from the SP's insurance carrier when losses are attributed to the SP. We show that the insurer cannot outperform the case where it underwrites both the SP and its customers. We use an actual cyber-insurance policy and claims data to calibrate and substantiate our analytical findings.

I. Introduction

Increasing costs emanating from cyber attacks and data breaches, such as legals fees, crisis management, business interruption, and ransom payments threaten organizations and businesses. To mitigate these losses organizations are increasingly turning to cyber-insurance in order to transfer some or all their risk to the insurer [1]. Like all other forms of insurance, cyber-insurance is primarily a method of risk transfer: a risk-averse insured pays an insurer a fixed premium in exchange for coverage in the event of a loss [2], [3].

But insurance carriers are also risk-averse, cost-minimizing agents that face multiple challenges. Not only must they effectively assess and differentiate risks of, and between, individual firms, but they must also manage systemic risk (also known as correlated or aggregate risk) across a portfolio of policies. Indeed, managing systemic risk is critical for insurance carriers because of how it can lead to catastrophic losses. And yet, insurance carriers still struggle to effectively identify indicators of systemic risk and understand how to manage their portfolio of policies to reduce their own costs [4]. Indeed, a major cause of systemic of risk is business interdependencies between organizations as

a result of outsourcing or supply chain relationships. In these cases the state of security of one firm depends not only on its own effort but also other firms' efforts [5]–[13], and in this world of increasing connectedness between today's businesses, risks can spill over easily and quickly from one firm to another. For instance, a breach at a credit card processing vendor can lead to major losses by retailers, or an outage at a network service provider (such as Amazon or Microsoft cloud services) can result in business interruption to a large number of customers. The denial of service attack against Dyn, an internet infrastructure (DNS) provider, caused some of the world's most popular websites including Netflix, Reddit, Twitter, and others, to be unavailable for most of one day in October 21, 2016 [14]. Moreover, this kind of risk dependency can lead firms to free ride off other firms' efforts and under-invest in security [15]–[17]. Of course, interdependent security arises not only in cybersecurity but also in financial networks [18], transportation systems [19], and cyber-physical systems [20].[1]

In particular, we consider two main reasons driving the concern over interdependent risk. First, it is more likely that simultaneous loss events could happen to interdependent agents, which would threaten the insurer's capital limit or other liquidity requirements. Second, in the event that a data breach or other loss events could be attributed to a third party, such as a service provider (e.g., a cloud platform vendor) who may be insured by a different carrier, the insurer of the primary party may seek to recover some or all of its losses from the third party's insurer/policy, thereby reducing its own risk exposure. If, on the other hand, the primary party's insurer underwrites both the primary firm, and its third party, then even if the loss to the primary could be attributed to the third party, the insurer would effectively be "suing itself" for the losses. All this has led to a strong desire among insurance carriers to minimize this type of risk dependency. However, a proper solution continues to elude the insurance carriers, reinsurers, and modeling firms [22].

It is thus of considerable interest to cyber-insurance underwriters to understand how to effectively manage not only individual firm risk, but overall portfolio risk in the presence of interdependent systems among policy holders. One device available to them is the ability to provide incentives (premium discounts) directly to firms that demonstrate improved security posture. While this may help reduce individual firm risk, it is unclear how this may help resolve systemic risk from interdependent business relationships.

Toward this end, the main purpose of this paper is to develop an understanding of the cyber-insurance market in the presence of interdependent (risk adverse) agents: a service provider and its customers. We use both analytic and computational techniques to model three portfolio alternatives available to the insurance carrier: insure just the service provider (*Portfolio type A*), insure both the service provider and its customers (*Portfolio type B*), or insure just the service provider's customers (*Portfolio type C*). These alternatives are depicted in Figure 1.

The strategic decision centers on how the insurer can induce the parties to reduce their risk while

[1]Another form of systemic risk can occur when a common vulnerability or system configuration shared across many policy holders may be exploited simultaneously, leading to multiple breaches, and subsequent insurance claims. Indeed, a number of past virus and trojan outbreaks in the past 20 years have been caused by exploiting a common vulnerability (e.g. Sasser, SQL Slammer). Similarly, the massive WannaCry and NotPetya ransomware attacks of 2016 were also caused by exploiting a common vulnerability across many firms [21]. Note, however, the focus of this paper concerns systemic risk caused by interdependent systems.

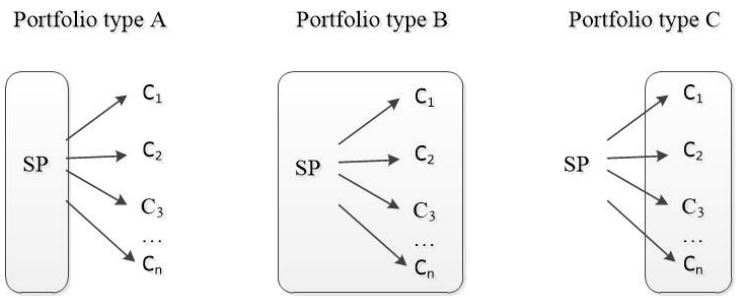


Fig. 1: Three Portfolio Types: shaded areas indicate entities insured by an underwriter.

maximizing its own profits. We examine how these incentives can be used to reduce the direct risk to one party, as well as to reduce indirect risks to dependent firms. We also examine social welfare implications and use data from an actual cyber-insurance policy, as well as one of the only sources of insurance claims data, to calibrate and substantiate our analysis. Our main findings are summarized as follows:

- Given the choice between insuring just a service provider (Portfolio A), or the service provider and all its customers (Portfolio B), an insurance carrier should choose Portfolio B. The reason is because the insurer can incentivize the service provider to improve its security posture in exchange for discounted premium. While this reduces the insurer's revenue from the service provider, it improves the security posture of the service provider and its customers, e.g., in the form of fewer business interruptions. We show that collectively this leads to lower overall risk, higher profits for the insurer and, higher social welfare relative to insuring just the service provider (Portfolio A).
- Given the choice between insuring both the service provider and its customers (Portfolio B), or just the service provider's customers (Portfolio C) and attributing losses to the service provider, an insurance carrier should choose Portfolio B. This is because with Portfolio C the insurer is unable to effectively induce the service provider to improve its security posture, which negatively affects all of its customers.
- If an insurer chooses to underwrite only the service provider's customers (Portfolio C), it should incorporate the risk condition of the service provider into the service provider's customers' premiums. By contrast, current practice often ignores the security posture of the service provide (or any third parties) when pricing the customer's policy.

Overall, our results suggest a novel and improved approach to cyber-insurance policy design that presents a new way of thinking about systemic risk and cyber risk dependency: to embrace and manage these risks, rather than avoid them. While we acknowledge the warranted caution against concurrent and correlated loss events, the emphasis of the present paper is to highlight a definitive silver lining behind risk dependency, and an opportunity to actively work toward reducing overall cyber risks in an ever-escalating and interconnected threat landscape.

II. Related Literature

Cyber-risk management has been studied extensively in the cybersecurity literature, such as cyber-insurance [23]–[25], cyber-risk forecast [26], and cybersecurity information sharing [27]–[30], to name a few. In particular, the body of theoretical scholarship on cyber-insurance has been growing steadily based on mechanism design and contract theory since the early 2000s, see e.g., [31], [32]. A number of studies focused on a monopolistic insurance market and showed that a monopolistic profit neutral cyber insurer can improve the network security as compared to no insurance scenario using premium discrimination [33]–[35], while others studied a competitive cyber-insurance market and showed that it is impossible to improve network security using a cyber-insurance contract [35], [36]. Furthermore, the problem of information asymmetry in cyber-insurance market has been studied in [37], [38]. For instance, [37] analyzed the questions that insurers ask to overcome information asymmetry and adverse selection issues. While foundational, none of these papers examined the issue of how an insurance carrier should respond to interdependent risks directly within its portfolio of policies.

More related to the present paper, previous work using a contract-theoretic approach [39] has shown that contrary to the common dependency-avoidance practice mentioned above, there is an unrealized incentive for an insurer to underwrite dependent risks. Paradoxically, the existence of risk dependency among a network of insureds allows the insurer to jointly design polices that incentivize the insureds to (collectively) commit to higher levels of effort, which can simultaneously result in improved state of security for all as compared to a portfolio of independent insureds, and in improved profits for the insurer. Related work examined whether these observations continue to hold when an insurer can recover a part of the loss suffered by an insured through a third-party liability clause when the loss can be attributed to another insured (the third party) underwritten by a different insurer [40]. Even with this loss recovery as an alternative, conditions exist where it is beneficial both from a security perspective and a profit perspective for an insurer to underwrite both interdependent insureds, precisely because this allows the insurer to control the risk dependency and incentivize both to commit to higher security efforts.

While [39], [40] used a rather simplified and stylized contract model somewhat detached from the actual insurance underwriting practice, in the present paper we adopt a standard underwriting framework commonly used in the insurance industry.

III. Computing Premiums Using Base Rates - Examples From An Actual Underwriter

In this section we briefly describe a common approach to calculating cyber-insurance premiums. The calculation begins by first selecting the *base premium* and a *base retention* (deductible) from previously defined lookup tables. The base premium is then modified through a linear product of additional factors. While different carriers use different values and types of factors in their premium expression, there are a number of commonly used factors.

Below, we provide an example of such a calculation using an actual cyber-insurance policy (see the Appendix to view the full rate schedule), with methods commonly found throughout the insurance industry. First, the base premium and retention are determined using table lookups, where the asset size (for financial institutions) or annual revenue (for non-financial institutions) of the insured maps to

assigned values, with both the rate and the retention amounts increasing in asset or revenue size. For instance, a financial institution of asset value up to \$100M would be charged a base rate of \$5,000 and base retention of \$25,000, while a firm of assets between \$500M and \$1B would be charged a base rate of \$11,000 and base retention \$100,000, all for a nominal coverage amount of \$1M. On the other hand, a non-financial firm with annual revenue between \$5M to \$10M would be charged a base rate of \$7,500 and base retention of \$25,000.

The base rate is then multiplied by a number of factors, with each factor modifying the base rate roughly between -20% and $+20\%$ with a few exceptions, as shown below.

- **Industry Factor:** Based on the type of business, an industry hazard is determined, with higher-risk businesses receiving a larger multiplier. For instance, agricultural and construction businesses receive the smallest hazard value (less risky) while web service providers receive the larger hazard value (more risky), as shown in Table I.

Industry	Factor
Agriculture	0.85
Construction	0.85
Not-for-Profit Organizations	1.00
Technology Service Providers	1.2
Telecommunications	1.2

TABLE I: Industry Hazard table

- **Retention Factor:** This factor depends on the retention (deductible) that the insured selects. Retention factor decreases as a function of the retention that the insured chooses, as shown in Table II.

Selected Retention	Base Retention			
	\$25,000	\$100,000	\$500,000	\$1000,000
\$25,000	**1.00**	1.16	1.34	1.47
\$100,000	0.87	**1.00**	1.16	1.27
\$500,000	0.75	0.87	**1.00**	1.10
\$1,000,000	0.68	0.79	0.91	**1.00**

TABLE II: Retention Factor

- **Increased Limit Factor:** This is a factor driven by the limit of the coverage: it is 1.0 if the insured accepts the default limit (corresponding to the base rate and base retention); it exceeds 1.0 if the insured wants to increase this limit, and falls below 1.0 if the insured asks for a lower coverage limit, as shown in Table III.
- **Co-insurance Factor:** This factor is less than 1.0 if the insured accepts to pay a share of the payment made against a claim. The value of this factor depends on the amount of the share that the insured accepts to pay. Table IV lists some of the co-insurance factors based on the co-insurance percentage.
- **Third-Party Modifier Factors:** This factor depends on the third party service provider. If the insured does not use any third party service, this factor is equal to 1.0. Otherwise, this factor is set

Coverage Limit	Increased Limit Factor
$1,000,000	1.000
$2,500,000	1.865
$5,000,000	2.987
$10,000,000	4.786
$25,000,000	8.925

TABLE III: Increased limit factor

Co-Insurance %	Co-insurance Factor
0%	1.000
1.0%	0.995
5.0%	0.980
10%	0.960
20%	0.920
50%	0.780

TABLE IV: Co-insurance factor

based on the third party service and the agreement between the insureds and the service provider, but is not a function of the security posture of the third-party.

- **Optional Coverage Grants:** In addition to the base coverage, the policy holder may purchase coverage for additional exposures, such as privacy costs or crisis management. Each additional coverage is calculated by multiplying the base rate by a number of factors including an option-specific modifying factor. For instance, the option of privacy notification expense uses a factor of 0.15, while the option of crisis management expense uses a factor of 0.02.

Note that other carriers use similar frameworks for calculating the final premium. We refer the interested reader to [1] for a more complete overview of current insurance policies. This multiplicative formula described above constitutes the basic model used for our analysis in the next section.

Example We complete this section by providing an example of how the final premium is calculated using the above tables. Consider a non-financial Technology Service Provider with annual revenue $6M who intends to purchase an insurance policy with retention $100,000, coverage limit $2.5M, and zero percent co-insurance. Moreover, this firm does not use any third party services; it wishes to opt in for additional coverage for privacy notification expense and crisis management expense. Based on the above tables, the following factors will be used in determining the total premium for this company:

- Base premium: $7,500; Base Retention: $25,000
- Industry Factor: 1.2 (Table I).
- Retention Factor: 0.87 (Table II).
- Limit Factor: 1.865 (Table III).
- Third-Party Modifier Factor: 1; Co-insurance Factor: 1 (Table IV).
- Privacy notification: 0.15.
- Crisis management: 0.02.

Therefore, the premium for this service provider is calculated as follows,

$$\begin{aligned} \text{Premium} &= 7500 \times 1.2 \times 0.87 \times 1.865 \times 1 \times 1 + 7500 \times (0.15 + 0.02) \\ &= 14602.95 + 1275 = \$15,877.95 \end{aligned} \tag{1}$$

IV. The Insurance Policy Model and Analysis

In this section we develop an expression for an insurance carrier's profit, modeled as a function of security incentives. We then compare the optimal amount of incentive and the carrier's profits between two cases: when it insures just the service provider (Portfolio A), and when it insures both the service provider and the provider's customers (Portfolio B).

A. Base premium calculation

Consider an insurer and its prospective insureds (the applicants), which include a service provider (SP, e.g. Amazon cloud services, or the third party) and its n customers. The insurer charges a base premium b_o to the service provider and base premium b_i to its customers i, $i = 1, 2, \cdots, n$.

As described, the base premium, b_i, depends on the total assets or revenue of the insureds. Moreover, the insurer asks the applicants to fill out a questionnaire describing their information security practices. Based on the completed questionnaire, the insurer modifies the base premiums by a factor f_i, $i = 0, 1, \cdots, n$, as described in the previous section. The insured pays $b_i \cdot f_i$ up front, and the insurer pays the insured $\max\{L_i - d_i, 0\}$ after a loss incident where L_i is a random variable denoting the loss amount of agent i and d_i is its elected retention/deductible. For the analysis that follows we ignore all the other factors unrelated to cybersecurity, as their inclusion (as additional multipliers) does not affect our model or our conclusion.

So far, the model does not consider dependent risks. Specifically, insured i's premium $b_i f_i$, $i = 1, \cdots, n$, is purely a function of its own security posture. While the information security questionnaire used to generate modifier factor f_i may include questions on whether i has a third party supplier, or whether it has proper procedures/policies in place in handling a third party, it does not directly assess the security posture of this specific third parties. This instead is assessed separately, given by f_o. We refer an interested reader to Questions 3-6 from the Chubb CyberSecurity policy shown in the appendix.

B. The security incentive modifier

We now introduce an incentive factor, f'_o, for the SP and subsequently examine its impact on the SP as well as its n customers. Specifically, suppose the insurer is willing to offer the SP a discount in premium in exchange for improved security posture as follows:

- The SP has an initially assessed premium $b_o f_o$, with a security modifier factor f_o.
- The SP agrees to invest more in security such that it could now be assessed at $\tilde{f}_o = f_o - f'_o$, for some $f'_o \in [0, f_o]$, i.e., a reduction in the modifier factor.
- In return, the insurer agrees to revise the premium to $b_o \tilde{f}_o$, reflecting a discount given the SP's improved security posture. Specifically, $b_o f'_o$ is the discount the SP receives.

Note that here for simplicity of presentation, we have assumed that the insurer is able to assess, and willing to match exactly in discount the amount corresponding to the reduced risk. That is, this SP now enjoys a revised premium equal to that which it would have received had it started at a security level measured at $\tilde{f}_o$ without the incentive. In practice the two need not be equal, i.e., the SP may require more or less in premium discount incentive to reach $\tilde{f}_o$. While this does not affect our qualitative conclusions, it does raise the interesting question as to whether in practice the incentive offered is sufficient for the SP to attain the corresponding risk reduction. In other words, could the SP take the discount amount $b_o f'_o$ and use it toward hiring additional personnel or purchasing products to achieve this goal? We will give an example in the context of the distributions used in our numerical analysis in Section V.

Our subsequent analysis focuses on whether a desirable operating point for the insurer is such that $f'_o > 0$, i.e., offering the incentive to the SP. Obviously, when there is no incentive, $\tilde{f}_o = f_o$, and the problem reverts to the original premium calculation.

C. Mapping security incentive to probability of loss

The security modifier factor f_i is tied to some underlying assumption of the probability of a cyber incident. This modifier can increase or decrease the base premium; the larger it is, the more likely is a loss event as estimated by the insurer. To the best of our understanding, by examining the rate schedules of many actual cyber-insurance policies, this factor itself is not directly tied to the magnitude of a loss; rather we believe the expected loss amount is factored into the base premium which is tied to the sector/industry and the size of the insured. The use of such a factor in the current underwriting practice would suggest that policies are risk priced in additional to being market priced (reflected in the base premium and retention). This aspect however does not affect our analysis since we only consider a single insurer.

To be concrete, let $P_o(\tilde{f}_o)$ denote the the probability of a breach to the SP, which is decreasing in the security incentive factor f'_o and increasing in the overall factor $\tilde{f}_o$. Similarly, we denote by $P_i(f_i)$, $i = 1, \cdots, n$, the probability of a loss incident of customer i *unrelated* to the SP. Both $P_o()$ and $P_i()$ are assumed to be increasing and differentiable. We will assume that if a breach happens to the SP, a business interruption (BI) or similar loss event occurs to its customer with probability t, also referred to as the level or degree of dependency. Further, we will assume that a business interruption induced by SP and the loss incident unrelated to the SP are independent events.

Putting these together, the probability of a loss event occurring to customer i is given by:

$$P_{li}(\tilde{f}_o, f_i) = P_i(f_i) + t \cdot P_o(\tilde{f}_o) - t \cdot P_o(\tilde{f}_o) \cdot P_i(f_i), \quad i = 1, \cdots, n \tag{2}$$

where the loss includes that due to the customer itself, due to business interruption brought on by the SP's breach, or both at the same time.

D. The insurer's profit function

Next, we define and compare the insurer's profit under two portfolio options: when it insures just the service provider (Portfolio A), and then when it insures both the service provider and its customers

(Portfolio B).

The insurer's profit (V_o) and expected profit ($\overline{V}_o$) from underwriting *just* the SP are defined as follows, both shown as functions of f'_o given that our focus is on this element under the insurer's control,

$$V_o(f'_o) = b_o \cdot (f_o - f'_o) - I_o \cdot (L_o - d_o)^+ \; ; \tag{3}$$

$$\overline{V}_o(f'_o) = E\{V_o(f'_o)\} = b_o \cdot (f_o - f'_o) - l_o \cdot P_o(f_o - f'_o) \; , \tag{4}$$

where $(x)^+ = \max\{x, 0\}$, L_o is the loss random variable, and $l_o = E((L_o - d_o)^+)$. Note that I_o is a Bernoulli random variable with parameter $P_o(f_o - f'_o)$.

We will assume the customers' security factors $f_i, i = 1, \cdots, n$ are uniformly distributed over some range $[f_{min}, f_{max}]$. The insurer's profit from customer i is then given by the following, again expressed as a function of the controllable f'_o:

$$V_i(f'_o) = b_i f_i - I_i \cdot (L_i - d_i)^+ \; ; \tag{5}$$

$$\overline{V}_i(f'_o) = b_i \cdot \frac{f_{min} + f_{max}}{2} - E_{f_i}[P_{li}(f_o - f'_o, f_i)] \cdot l_i \; , \tag{6}$$

where L_i is the loss random variable of customer i. Again, I_i is a Bernoulli random variable with parameter $P_{li}(f_o - f'_o, f_i)$ and $l_i = E((L_i - d_i)^+)$.

If the insurer chooses to underwrite *both* the SP and its n customers then its expected total profit is given by,

$$\overline{V}_{total}(f'_o) = \overline{V}_o(f'_o) + \sum_{i=1}^{n} \overline{V}_i(f'_o) \; ; \tag{7}$$

$$\overline{V}_{max} = \max_{f'_o} \; \overline{V}_{total}(f'_o) \; . \tag{8}$$

E. Analysis of the optimal incentives and carrier profits

Now that we have established expressions for the carrier's profits as a function of security incentives, we next seek to answer two questions: first, what security incentives should the carrier provide the service provider, and secondly, which portfolio strategy yields the highest profit?

We have defined $P_o(\tilde{f}_o)$ to be an increasing function of $\tilde{f}_o$, implying that $P_o(f_o - f'_o)$ is a decreasing function of the incentive f'_o. We assume this to be a strictly convex function of f'_o, reflecting a decreasing marginal return on effort. Note that it is widely accepted to model loss probability as a function of the security investment, see e.g., [15], [41]–[43]. Our model here is consistent with this literature since we have assumed that the incentive factor f'_o is proportional to security effort/investment, while allowing us to highlight and express this function in terms of the carrier's controllable in this underwriting framework.

Our first result compares the optimal incentive that an insurance carrier would offer the SP when insuring just the SP (Portfolio A), and insuring both the SP and its customers (Portfolio B). That is, we compare the optimal incentive factor f_o^* that maximizes $\overline{V}_o()$, with the optimal incentive factor f_o^{**} that maximizes $\overline{V}_{total}()$.

Theorem 1: Under the assumption that $P_o(f_o - f'_o)$ is decreasing and strictly convex in f'_o, we find that $f_o^* \leq f_o^{**}$, where $f_o^* = \arg\max_{f'_o} \overline{V}_o(f'_o)$ and $f_o^{**} = \arg\max_{f'_o} \overline{V}_{total}(f'_o)$. In other words, the

underwriter offers a higher incentive to the SP when insuring all parties, compared with the incentive offered to the SP as the only insured.

Proof 1: The insurer's profit of underwriting the service provider and the customers is given by:

$$\begin{aligned}\overline{V}_{total}(f_o') &= \overline{V}_o(f_o') + \sum_{i=1}^{n}\overline{V}_i(f_o') \\ &= b_o\cdot(f_o - f_o') - l_o P_o(f_o - f_o') + \sum_{i=1}^{n} b_i \frac{f_{min}+f_{max}}{2} \\ &\quad -l_i\cdot P_o(f_o - f_o')\cdot(t - tE[P_i(f_i)]) - l_i\cdot E[P_i(f_i)]\ . \end{aligned} \tag{9}$$

Using the first order optimality condition, we have

$$\frac{\partial \overline{V}_{total}(f_o')}{\partial f_o'} = 0 \tag{10}$$

$$\Rightarrow \qquad f_o^{**} = \left(f_o - (P_o')^{-1}\left(\frac{b_o}{[l_o + \sum_{i=1}^{n} l_i\cdot(t - t\cdot E(P_i(f_i)))]}\right)\right)^{+}\ . \tag{11}$$

Similarly, we can find the optimal value f_o^* that maximizes $\overline{V}_o$:

$$\begin{aligned}&\frac{\partial \overline{V}_o}{\partial f_o'} = -b_o + l_o\cdot P_o'(f_o - f_o') = 0 \\ \Rightarrow \qquad &\arg\max_{f_o'} \overline{V}_o(f_o') \in \left(f_o - (P_o')^{-1}(\frac{b_o}{l_o})\right)^{+} \\ \Rightarrow \qquad &f_o^* = \left(f_o - (P_o')^{-1}(\frac{b_o}{l_o})\right)^{+}\ . \end{aligned} \tag{12}$$

Because $P_i^{'}()$ is an increasing function and $\frac{b_o}{l_o} > \frac{b_o}{[l_o+\sum_{i=1}^{n} l_i\cdot(t-t\cdot E(P_i(f_i)))]}$, we have $f_o^* \le f_o^{**}$. ■

Theorem 1 suggests that if the insurer underwrites both the SP and its customers (Portfolio B), it benefits from a better state of security (induced by higher incentive to the SP) as compared to the optimal level if it only underwrites the SP (Portfolio A).

Furthermore, if the parameters such as b_i and l_i are such that $\overline{V}_i(f_o^*) > 0$ (i.e., there is expected profit from any single policy when the SP is incentivized at the level f_o^*; this need not be true if b_i is too small and l_i too large, in which case a rational insurer would not underwrite the policy), then we also have the following:

$$\overline{V}_{total}(f_o^{**}) \underbrace{\geq}_{\text{by the optimality } f_o^{**}} \overline{V}_{total}(f_o^*) \underbrace{\geq}_{\text{by the positivity of } \overline{V}_i(f_o^*)} \overline{V}_o(f_o^*)\ . \tag{13}$$

And similarly,

$$\overline{V}_{total}(f_o^{**}) \underbrace{\geq}_{\text{by the optimality } f_o^{**}} \overline{V}_{total}(f_o^*) \underbrace{\geq}_{\text{by the positivity of } \overline{V}_i(f_o^*)} \overline{V}_i(f_o^*) \ge \overline{V}_i(0)\ , \tag{14}$$

where the last inequality results from the fact that the risk sustained by customer i is lower when the SP is incentivized at any level $f_o^* > 0$.

The above result suggests that at the right level of incentive for the SP, the insurer enjoys greater profits by insuring both the SP and its customers (Portfolio B), relative to insuring just the SP (Portfolio A), or any subset of its customers.

F. Third-party liability

Next we consider third-party liability. This refers to the ability of an injured party to seek redress for losses from an injurer, and is a coverage category commonly found in insurance policies. In the context of our study, this implies that if a firm suffers loss due to business interruption brought on by a breach at its SP, the firm's insurance carrier can, on the firm's behalf, seek redress from the SP's insurer. However, if the same carrier were to underwrite both the firm and the SP, such compensation would obviously not occur. In one of the few datasets that reports actual cyber-insurance claims data, NetDiligence [44] shows that 13% of all data breaches and cyber incidents can be attributed to a third party. Accordingly, we will use a parameter q to represent the probability that a loss can be attributed to a SP.

We define U as the insurer's profit when it underwrites only the SP's customers (Portfolio C). We have:

$$\begin{aligned} U_i(f_o') &= b_i \cdot f_i - J_i \cdot (L_i - d_i)^+; \\ \overline{U}_i(f_o') &= E[U_i(f_o')] \\ &= b_i \cdot f_i - (E[P_i(f_i)] + (1-q) \cdot \left[tP_o(f_o - f_o') - E[P_i(f_i)]tP_o(f_o - f_o')\right])l_i \ , \end{aligned} \tag{15}$$

where J_i is a Bernoulli random variable with parameter $P_i(f_i) + (1-q) \cdot [tP_o(f_o - f_o') \cdot (1 - P_i(f_i))]$; this is the probability that a loss incident happens to customer i and *cannot* be attributed to the SP. In this case the SP is insured by another carrier, referred to as the third-party insurer, whose profit is given by:

$$U_o(f_o') = b_o(f_o - f_o') - I_o \cdot (L_o - d_o)^+ - \sum_{i=1}^{n} K_i \cdot (L_i - d_i)^+; \tag{16}$$

$$\begin{aligned} \overline{U}_o(f_o') &= E[U_o(f_o')] \\ &= b_o \cdot (f_o - f_o') - P_o(f_o - f_o') \cdot l_o - \sum_{i=1}^{n} q \cdot \left[tP_o(f_o - f_o')\right] \cdot [1 - E[P_i(f_i)]]\, l_i \ , \end{aligned} \tag{17}$$

where K_i is a Bernoulli random variable with parameter $q \cdot [tP_o(f_o - f_o')] \cdot [1 - P_i(f_i)]$; this is the probability that a loss incident happens to customer i and it *can* be attributed to the third party successfully. Here we have assumed that whenever losses can be attributed to the SP, the customer's insurer (also referred to as the primary insurer) is fully reimbursed. However, our result in Theorem 2 remains valid for partial or fractional compensation as well.

Next, we compare the insurer's profit from underwriting only the SP's customers (with the possibility of recovering losses from the SP's insurer) (Portfolio C), with its profit from underwriting both the SP and its customers (Portfolio B).

We denote the insurer's profit from underwriting only the SP's customers as $\overline{U}_{max} = \sum_{i=1}^{n} \overline{U}_i(f_o^\star)$, where $f_o^\star = \arg\max_{f_o'} \overline{U}_o(f_o')$, and denote the insurer's profit from underwriting both the SP and its customers as $\overline{V}_{max}$ from Eqn. (8), where the maximum is attained at $f_o^{\star\star}$.

Theorem 2: At the right level of incentive for the SP, the insurer enjoys greater profit by insuring both the SP and its customers (Portfolio B), rather than just the SP's customers (Portfolio C). That is, $\overline{V}_{max} \geq \overline{U}_{max}$, where $\overline{V}_{max} = \overline{U}_o(f_o^{\star\star}) + \sum_{i=1}^{n} \overline{U}_i(f_o^{\star\star})$, and $\overline{U}_{max} = \sum_{i=1}^{n} \overline{U}_i(f_o^\star)$. Moreover, given that $P_o(f_o - f_o')$ is decreasing and convex in f_o', we have $f_o^\star \leq f_o^{\star\star}$, which implies that the state of security improves for both the SP and its customers when the insurer underwrites both.

The first part of the above result is rather trivial: if the primary insurer is compensated by the third-party insurer, it must therefore be profitable to underwrite the SP (otherwise the SP would not be able to obtain a policy in the first place). Thus the insurer of the SP's customers can only gain by insuring the SP itself.

The second part of the result is more interesting and less straightforward. The intuition is that when the insurer underwrites both the SP and its customers (Portfolio B), it is in its best interest to provide stronger incentive to the SP in an attempt to reap the multiplicative effect of risk reduction of the SP on its customers, i.e., the positive externality. In summary, by embracing the risk dependency, the insurer not only gains but also contributes to social welfare.

V. Numerical Examples

In this section we examine closely a number of numerical examples that put the preceding analytical results into context. To do so, we will need to substantiate two elements of our model: the relationship between the security modifying factor, i.e., the function $P(f)$, and the loss distribution governing L. We will also use base premium and retention values found in Section III.

A. Examples of the loss probability function

We present three examples of $P_o(f_o - f_o')$ as a function of f_o' while fixing $f_o = 1.2$ and $b_o = 52000$; these are illustrated in Figure 2 and used later in this section to perform numerical analysis.

$$P_o(f_o - f_o') = \frac{0.05}{\frac{b_o(1.2-(f_o-f_o'))}{1000} + 1} \tag{18}$$

$$P_o(f_o - f_o') = \frac{0.05}{(1 + \exp(\frac{b_o \cdot (1.2-(f_o-f_o'))}{1000} - 20))} \tag{19}$$

$$P_o(f_o - f_o') = \frac{5}{1000} + 0.05 \cdot \exp(-\frac{b_o \cdot (1.2 - (f_o - f_o'))}{1000}) \tag{20}$$

The choice of these functions are somewhat arbitrary: the main intent is to capture a few families of decreasing functions with subtle yet significant differences as explained below, while noting that our conclusion and results hold more generally. More specifically:

- The loss given in Eqn (18) (the blue curve) is simply a decreasing, convex function which indicates that initial effort in risk reduction results in larger marginal benefits in loss reduction, but that the loss probability will continue to decrease at a diminishing rate. This would apply to a typical firm

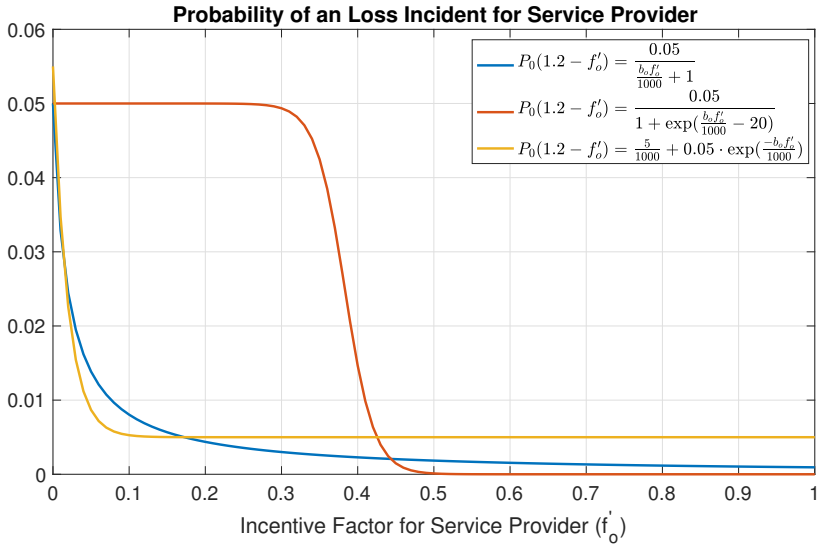


Fig. 2: $P_o(1.2 - f'_o)$, the probability of a loss event to the SP

whose initial investment (say in firewall) is very effective, after which more expensive products (e.g., intrusion detection) continue to reduce risk but the return on investment becomes lower.

- The loss in Eqn (19) (the red curve) suggests the initial effort has to be significant enough (exceeding a threshold) to have any appreciable effect on loss reduction. Equivalently, this may be viewed as modeling a type of firms that only respond to incentives when they are substantial or reach a tipping point. Beyond this, the curve similarly exhibits diminishing returns. Note that this loss function is not convex but we show in the appendix the result of theorem 1 holds in this case as well.
- Finally, the loss in Eqn (20) (the yellow curve) illustrates a scenario where the reduction in loss initially behaves similarly to the first case, but reaches a maximum at a point beyond which no amount of effort can further reduce. This is meant to capture the scenario where external factors beyond the insured's control is at significant play, contributing to a non-zero "floor" in the probability of a loss event. This could apply to the case where there is persistent susceptibility to social engineering that no amount of investment or training can completely remove; or, where the firm is simply not able to address all security challenges.

It should be noted that the above examples serve to illustrate the different ways loss probabilities may change as incentives/security investments increase. The actual values used may or may not accurately reflect reality. For instance, in reality the scale of the loss probability could be orders of magnitude larger (0.1 instead of 0.01) or smaller (0.001 instead of 0.1). Unfortunately there is no publicly available data that would allow us to calibrate; as already mentioned, it is unclear how these factor values were derived by an underwriter in the first place.

B. Examples of the loss distribution

We will use data reported in the cyber-insurance claims study by NetDiligence [44] to obtain breach loss distributions, summarized in Table V. The "Mid Revenue" range contains somewhat unexpected small median and mean values. This appears to be an anomaly: since the sample sizes (number of cases) are small, an oversized or undersized breach can significantly throw off the average.

	Cases	Median ($)	Mean ($)
Nano Revenue (< $50M)	52	49,000	215,297
Micro Revenue ($50M - $300M)	31	88,154	487,411
Small Revenue ($300M - $2B)	15	118,671	599,907
Mid Revenue ($2B - $10B)	9	91,457	173,851
Large-Revenue ($10B - $100B)	8	3,326,313	5,965,571

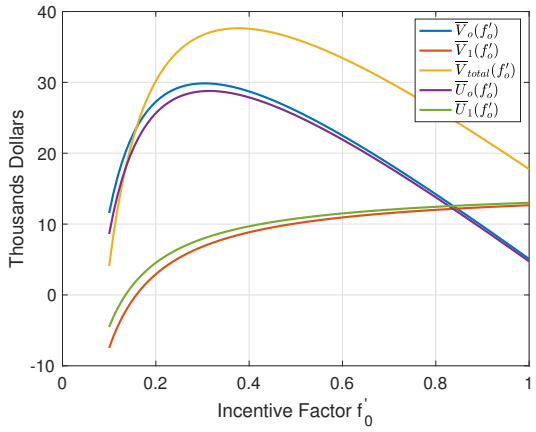
TABLE V: Cost of data breach between 2016-17 organized based on the breached firm's revenue

C. Example 1: A service provider and a customer with large revenue

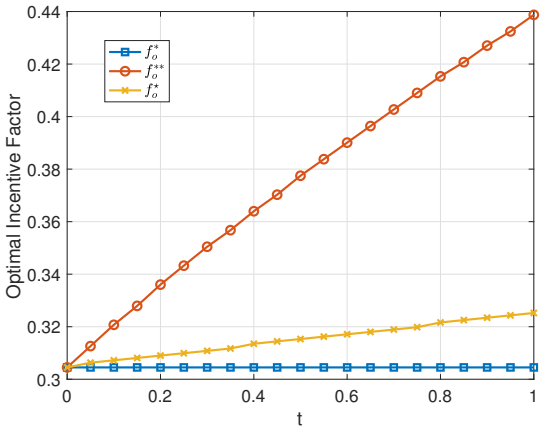
In this example, we consider a SP and a single customer, both of large revenue (e.g., a major web hosting provider and a large corporate customer). Using the rate schedule provided in III, we will set the base premium and base retention for the SP and its customer to be $b_o = b_1 = \$52,000$ and $d_o = d_1 = \$250,000$, respectively. We consider the following loss function for the customer: $P_1(f_1) = \frac{0.05}{\frac{b_1\cdot(1.2-f_1)}{1000}+1}$. Moreover, factor f_1 is uniformly distributed over $[0.6, 1.2]$ and as mentioned this depends on the outcome of its information security questionnaire.

Using the NetDiligence data, we will assume that both L_o and L_1 are log-normally distributed with a mean of $5,965,571 and median $3,326,313. Moreover, as mentioned earlier NetDiligence reports that 13% of data breaches can be attributed to a third party; we will accordingly set $q = 0.13$. We will assume that the SP was assessed with $f_o = 1.2$ and the dependency parameter is $t = 0.5$.

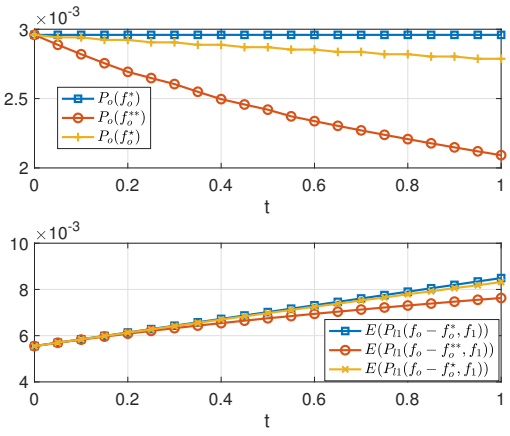
We will first consider $P_o(f) = \frac{0.05}{\frac{52000\cdot(1.2-f)}{1000}+1}$, with results shown in Figure 3. Specifically, Figure 3a illustrates insurer's profit as a function of f'_o. In this example, $f_o^* = 0.3054$, $f_o^{**} = 0.3775$, $f_o^\star = 0.3153$. Note that the insurer's total profit at f_o^* is $\overline{V}_o(f_o^*)+\overline{V}_1(f_o^*) = \$36,637$ and at f_o^{**} it is $\$37,792$, a roughly $\$1,000$ gain by taking the risk dependency into account and offering jointly optimal policies to the SP and the customer. Moreover, 3a shows that by insuring only the customer and getting compensation from the SP's policy, the insurer cannot make more profit as compared to insuring both: $\overline{V}_1(f_o^\star) = \$8,152 < \overline{V}_o(f_o^{**}) + \overline{V}_1(f_o^{**}) = \$37,473$. Figure 3b and 3c plot the optimal incentive factor and the probability of a loss event to the SP and its customer, respectively, as a function of the dependency t. If the insurer underwrites only the SP (Portfolio A, blue line), t does not factor into the policy decision and thus the insurer will not offer any incentive to the SP. On the other hand, if the insurer underwrites both, then offering incentive to the SP is now in its interest, and the incentives increases as t increases (Portfolio B, orange line). Finally, if an insurer underwrites only the SP and pays the third-party compensation for its customer's loss (yellow line), the incentive factor is also increasing as a function of t but it increases slower than f_o^{**}. Figure 3d shows how much can be gained by taking



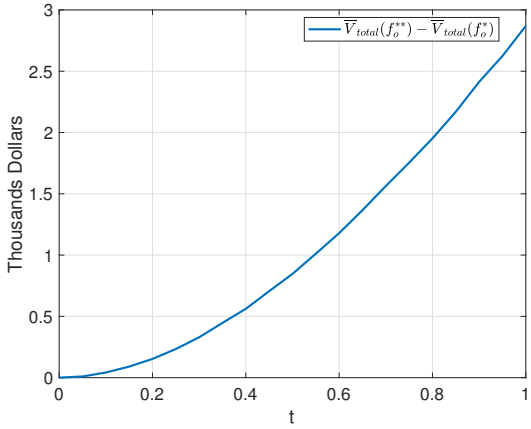
(a) Profit of the insurer as a function of f'_o



(b) Optimal Incentive Factor as a function of t



(c) Probability of a loss incident as a function of t



(d) Profit gain as a function of t

Fig. 3: Insurer's profit and probability of a loss incident under loss model (18).

risk dependency into account, and the higher the dependency the more the insurer stands to gain by jointly designing contracts for both the SP and its customer.

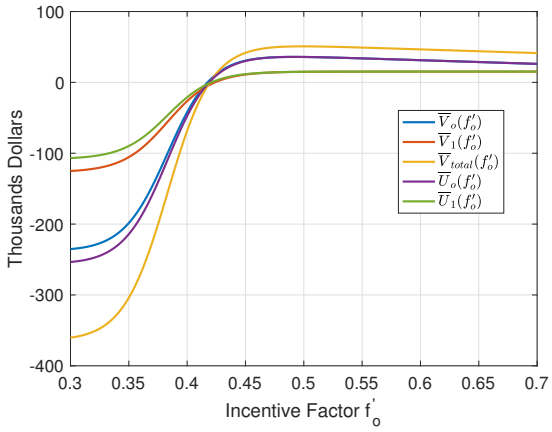
The case $P_o(f_o - f'_o) = \frac{0.05}{(1+\exp(\frac{b_o(1.2-(f_o-f'_o))}{1000}-20))}$ is shown in Figure 4. Specifically, Figure 4a illustrates insurer's profit as function of f'_o. In this example, $f_o^* = 0.4913$, $f_o^{**} = 0.4991$, $f_o^\star = 0.4925$.

Finally the case $P_o(f_o - f'_o) = \frac{5}{1000} + 0.05\exp(-\frac{b_o(1.2-(f_o-f'_o))}{1000})$ is shown in Figure 5. In this example, $f_o^* = 0.1084$, $f_o^{**} = 0.1161$, $f_o^\star = 0.1096$.

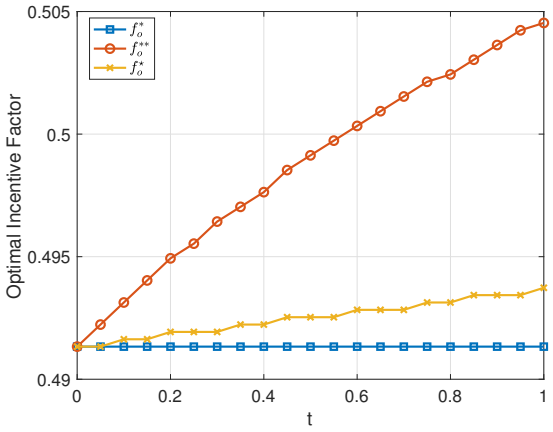
D. Example 2: An SP and multiple customers with smaller revenue

In this example, we consider an SP and n customers with relatively smaller revenue.

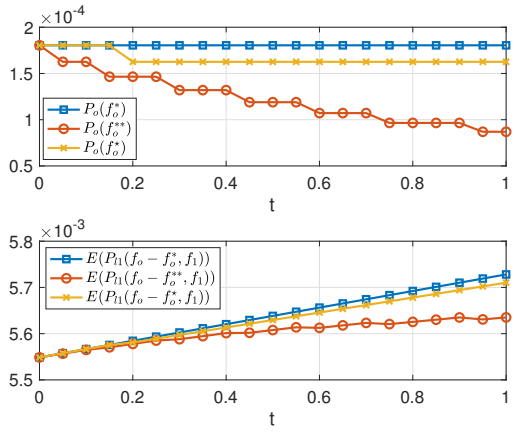
Again, using the rate schedule provided in III, we will set the base rate and retention for the customers at $b_i = \$5,000$, $d_i = \$25,000$, $i = 1, \cdots, n$. The factors f_i, $i = 1, \cdots, n$ are drawn uniformly from $[0.6\ ,\ 1.2]$. Using Table V, the loss random variable L_i, $i = 1, \cdots, n$ has a mean and median of \$599,907 and \$118,671, respectively. Similar as in the previous example, the mean and median of loss L_o are set at \$5,965,571 and \$3,326,313, respectively. We again assume that L_i follows a log-normal



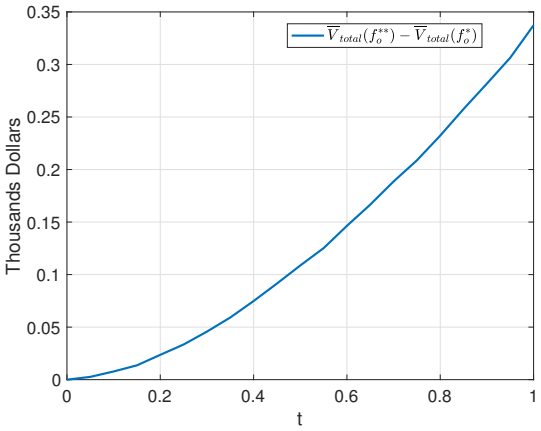
(a) Profit of the insurer as a function of f'_o



(b) Optimal incentive factor as a function of t



(c) Probability of a loss incident as function of t

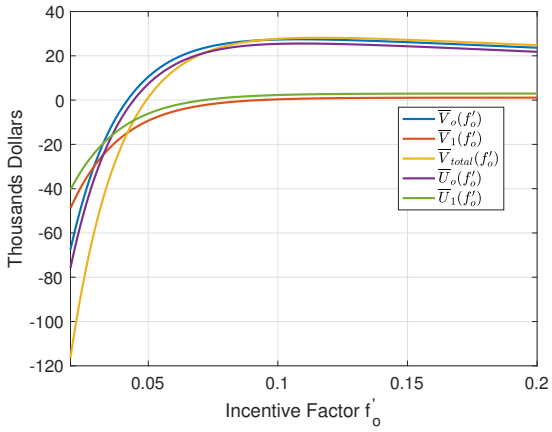


(d) Profit gain as function of t

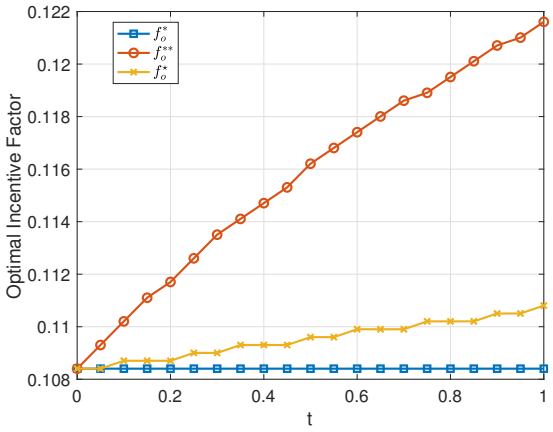
Fig. 4: Insurer's profit and probability of a loss incident under loss model (19)

distribution. In addition, we set $f_o = 1.2$, $t = 0.5$, and $q = 0.13$. Compared to the previous example, in this example we shall also examine the effect of the number of customers (n) on the optimal policy. Moreover, we consider the following loss function for customer i: $P_i(f_i) = \frac{0.05}{\frac{5000(1.2-f_i)}{1000}+1}$. The results are shown in Figure 6.

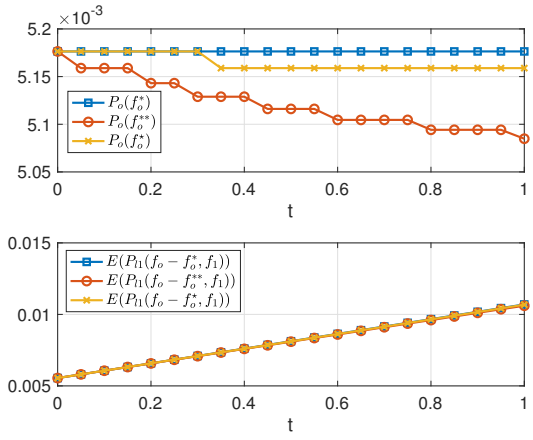
Figure 6a illustrates the optimal incentive factor f_o^{**} as a function of n. This plot implies that as the number of customers increases, the insurer would incentivize the SP more. The reasons behind this is obvious: since the risk spill over now impact more customers the more the SP can reduce its risk, the more upstream benefit the insurer attains (e.g., in much reduced business interruptions). Specifically, given that a breach occurred to the SP, the probability of no upstream business interruption is given by $1-(1-t)^n$, which an increasing function of n. Thus it is in the insurer's interest to reduce the likelihood of loss on the part of the SP. As a result, f_o^{**} is increasing as function of n, while f_o^* is independent of n as it maximizes only $\overline{V}_o$. Moreover, Figure 6a implies that $f_o^\star$ is also increasing as a function of n. Figure 6b implies that if the insurer does not gain by underwriting the customers and attributing all or a part of the loss to the SP as compared to the profit by underwriting all of them; we



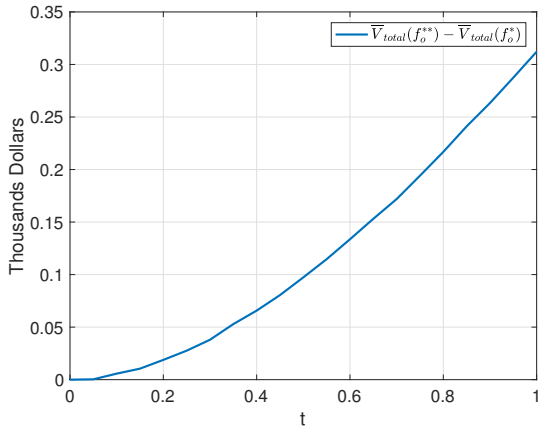
(a) Profit of the insurer as a function of f'_o



(b) Optimal Incentive Factor as a function of t



(c) Probability of a loss incident as function of t



(d) Profit gain as function of t

Fig. 5: Insurer's profit and probability of a loss incident under loss model (20)

see in some cases the third party's insurer has negative expected profit, in which case a policy is not viable.

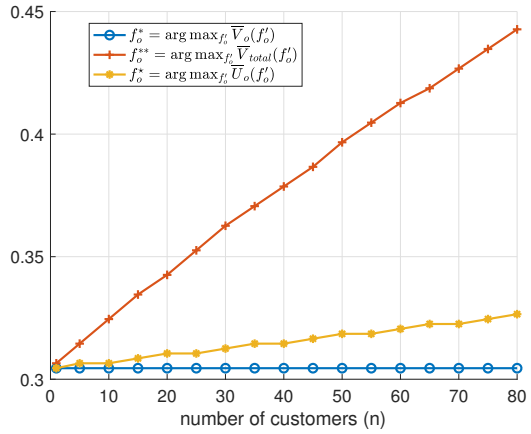
Figures 7 and 8 shows similar results for the other two loss functions $P_o(f_o - f'_o) = \frac{0.05}{(1+\exp(\frac{b_o(1.2-(f_o-f'_o))}{1000}-20))}$ and $P_o(f_o - f'_o) = \frac{5}{1000} + 0.05 \cdot \exp(-\frac{b_o \cdot (1.2-(f_o-f'_o))}{1000})$.

VI. Discussions

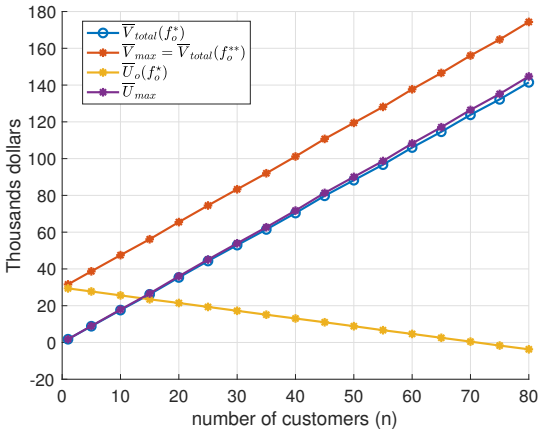
We now discussion further three aspects of the model studied in this paper.

A. *Is the premium discount sufficient?*

Let's consider a non-financial technology service provider firm with annual revenue between \$5M and \$10M. In this case, the base premium $b_o = \$7,500$. We will assume the firm is assessed with $f_o = 1.2$. Now assume that the insurer sets the incentive factor f'_o to be 0.35. Therefore, the firm pays $b_o \cdot (f_o - f'_o) = \$6375$ as the premium, after receiving $b_o \cdot f'_o = \$2625$ in discount. Using salary surveys such as [45], let's consider an IT security personnel who has a bachelor's degree, 5 years of

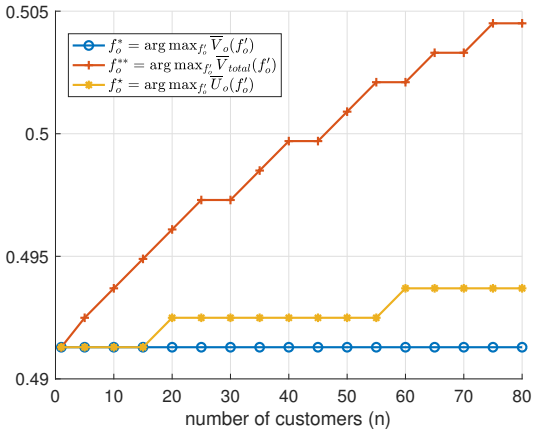


(a) Profit of the insurer as a function of f_o'

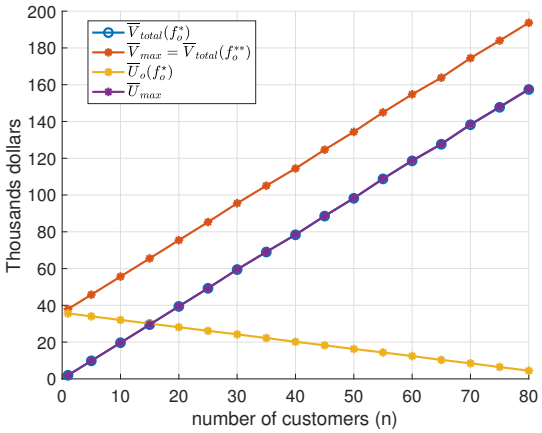


(b) Probability of a loss incident as function of t

Fig. 6: Insurer's profit and probability of a loss incident under loss model (18)



(a) Profit of the insurer as a function of f_o'



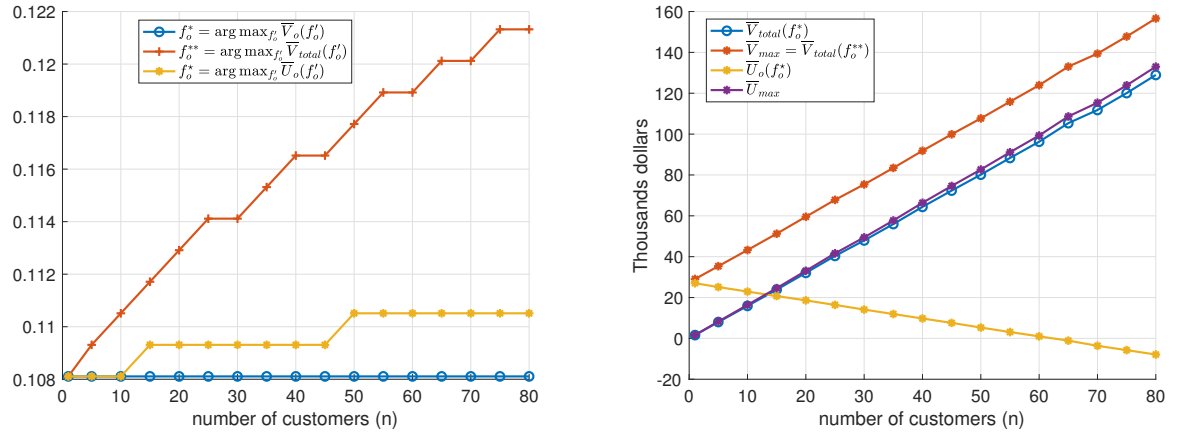
(b) Probability of a loss incident as function of t

Fig. 7: Insurer's profit and probability of a loss incident under loss model (19)

experience, and commands a salary of \$85K. The premium discount the firm receives can be translated into a fraction of this person's compensation:

$$\frac{\$2625}{\$85000} \times 50 \text{ working weeks } = 1.5 \text{ weeks.} \tag{21}$$

Therefore, the incentive provided by the underwriter is just enough to hire an experienced person for 10 days. It is debatable whether this amount of investment in security is adequate to reduce the firm's cyber risk (by 10^{-9} according to Model (19), or by 0.05 according to Model (20), by setting $b_o = \$7,500$ in each, respectively). A potential mismatch between what this analysis suggests and reality may be attributed to two factors. Firstly, as already mentioned, the loss values shown in Fig 2 could be orders of magnitude different from reality; in other words, if the risk reduction is from a breach probability of 0.1% to 0.07%, then perhaps 10 days' worth of work (say in deploying software patches)



(a) Profit of the insurer as a function of f_o'

(b) Probability of a loss incident as function of t

Fig. 8: Insurer's profit and probability of a loss incident under loss model (20)

is sufficient. Secondly, it may also be argued that the current levels of base premium is inconsistent with the underlying cyber risk (and what it takes to reduce the risk) to begin with.

B. Social welfare

Our study so far has focused on whether it is in the interest of an underwriter to insure risk-dependent insureds, and if so how best to do so. We now turn to the issue of social welfare, i.e., whether by embracing risk dependency the underwriter can also help improve the total utility. We have shown that underwriting both SP and its customers and giving SP more discount on premium improves the insurer profit and decreases the probability of data breach. As a consequence of the latter, the utility of the insureds improves; thus underwriting both SP and its customers improves the social welfare (total utility) in general. Below we use an example similar to that provided in Section V-C to illustrate this.

Consider an SP and a single customer, and assume that both have a large annual revenue ($10B-$100B), with a base rate $b_o = b_1 = \$52,000$ and base retention $d_o = d_1 = \$250,000$. We assume that $f_o = 1.2, f_1 = 1$ and $P_o(f) = P_1(f) = \frac{0.05}{1+\frac{b_o(1.2-f)}{1000}}$ and $t = 0.5$. Based on Table V, we assume both L_o and L_1 have log-normal distribution with mean $5,965,571 and median $3,326,313.

We now compare two cases. In the first case the insurer ignores the risk dependency and attempts to separately maximize its profit from the SP and its customer, respectively. In the second case the insurer jointly optimizes the two policies.

In the first case, the insurer obtains the discount to the SP as follows:

$$\begin{aligned} l_o = l_1 &= E((L_o - d_o)^+) = \$5,715,600 \\ \overline{V}_o(f_o') &= b_o \cdot (f_o - f_o') - l_o P_o(f_o - f_o') \Rightarrow f_o^* = 0.3045 \end{aligned} \tag{22}$$

The insurer's profit and the insureds' costs are as follows:

- Insurer's total expected revenue: $V_{total}(f_o^*) = \$48,629$.

- SP's expected cost:

$$b_o \cdot (f_o) + E\{D_o\}P_o(f_o - f_o^*) = +52000 \times 1.2 + 28753 \times 0.003 = \$62,486$$

- SP's customer's expected cost:

$$b_1 \cdot f_1 + E\{D_1\} \cdot P_{l1}(f_o - f_o^*) = 52000 \times 1 + 28753 \times 0.0058 = \$52,167$$

- Total utility (revenue less cost):

$$48629 - 62486 - 52167 = -\$66,024$$

Here $D_i = \begin{cases} L_i \text{ if } L_i \leq d_i \\ d_i \text{ o.w} \end{cases}$ is the amount of deductible that insured i pays. Note that we do not consider discount $b_o \cdot f_o^*$ in the SP's costs because this is assumed to be used toward its security investment.

In the second case the insurer jointly maximizes the profit from the SP and its customer. It obtains the optimal incentive factor as follows:

$$\overline{V}_{total}(f_o') = b_o \cdot (f_o - f_o') - l_o P_o(f_o - f_o') + b_o(f_o - f_o') + b_1 \cdot f_1 - P_{l1}(f_o - f_o')l_1 \Rightarrow f_o^{**} = 0.3773$$

The insurer's profit and the insureds' costs are given by:

- Insurer total expected revenue: $V_{total}(f_o^{**}) = \$49,481$.
- SP's expected cost:

$$b_o(f_o) + E\{D_o\}P_o(f_o - f_o^{**}) = 52000 \times 1.2 + 28753 \times 0.0024 = \$62,469$$

- SP's customer expected cost:

$$b_1 f_1 + E\{D_1\} \cdot P_{l1}(f_o - f_o^{**}) = 52000 \times 1 + 28753 \times 0.0056 = \$52,161$$

- Total utility (revenue less cost):

$$49481 - 62469 - 52161 = -\$65,149$$

We see that the total utility or social welfare is higher in the second case, when the insurer takes risk dependency into account and jointly optimizes the two policies. It is interesting to note that the values used in this example lead to negative social welfare, i.e., the total cost born by the insureds exceeds the total profit made by the insurer. The negative total utility is a reflection of the damage inflicted by attackers behind data breaches.

C. Modeling third party liability

We have assumed that the probability that the insurer can attribute a part of the loss to the third party is a constant (q) and is independent of P_o and P_i and t. An alternate model is to find probability q using P_o, P_i and t. Let q_i be the probability that the insurer of insured i can attribute a part of the loss to its third party. Moreover, define events A_i and B_i as follows,

- A_i: a business interruption occurs to insured i due to a data breach/loss incident on the SP's side.
- B_i: a loss incident occurs to insured i.

We then have:

$$\begin{aligned} &Pr\{A_i \cap B_i\} = P_o(f_o - f_o') \cdot (1 - P_i(f_i)) \\ &P\{B_i\} = P_{li}(f_o - f_o', f_i) = P_i(f_i) + t \cdot P_o(f_o - f_o') - t \cdot P_o(f_o - f_o') \cdot P_i(f_i) \\ &q_i = Pr\{A_i | B_i\} = \frac{Pr\{A_i \cap B_i\}}{Pr\{B_i\}} = \frac{P_o(f_o - f_o') \cdot (1 - P_i(f_i))}{P_i(f_i) + t \cdot P_o(f_o - f_o') - t \cdot P_o(f_o - f_o') \cdot P_i(f_i)} \end{aligned} \tag{23}$$

We can show that under this model Theorem 2 continues to hold.

VII. Conclusion

In this paper, we applied a principal and agent modeling approach to understanding how an insurance carrier can best manage its portfolio risk of cyber-insurance policies, given interdependent risks across the insureds. We used a typical base rate approach to pricing premiums, and incorporated additional datasets to calibrate our model.

We believe our results are significant because they suggest an alternative and preferred decision strategy for the carrier. First, we found that insuring interdependent agents (SP and its customer) leads to higher profit, compared with not insuring them simultaneously, the reason being that the insurer can incentivize the SP to increase its security level by offering a discount on its premium. When SP provides more secure services for its customers, the chance of business interruption for the customers decreases significantly and the insurer's profit improves. In other words, receiving premiums from all interdependent agents and paying less in coverage due to high security level drives the profit opportunity not present in insuring interdependent agents.

In addition, we considered a scenario where the insurer underwrites only the SP's customers (Portfolio C) and is able to attribute a part of the loss to the SP and receive compensation from SP's insurer due to the third party liability. In this case, the insurer's profit decreases compared with the scenario of insuring both the SP and its customers (Portfolio B). The reason is that the insurer loses the SP's premium and the insurer cannot incentivize the SP to decrease the chance of business interruption for SP's customers. These results are different from conventional wisdom that the insurers avoid insuring interdependent agents.

Finally, we confirmed our results and theorems by providing numerical example using real data. Moreover, we showed the effect of interdependency t on insurer's decision. As the SP and its customers become more interdependent, the insurer must incentivize the SP more in order to use the profit opportunity.

In conclusion, we believe that these results will help insurance carriers better understand and manage this critical issue of systemic risk.

Acknowledgment

This work is supported by the NSF under grant CNS-1422211, CNS-1616575, CNS-1739517, and by the DHS via contract number HSHQPM17X00233.

REFERENCES

[1] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, "Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?" 2017.

[2] 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 *Decision and Game Theory for Security*, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauer, Eds. Cham: Springer International Publishing, 2017, pp. 519–532.

[3] D. T. Hoang, D. Niyato, and P. Wang, "Optimal cost-based cyber insurance policy management for mobile services," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Sept 2017, pp. 1–5.

[4] "Understanding systemic cyber risk," in *Global Agenda Council on Risk and Resilience,World Economic Forum*, Oct 2016.

[5] R. A. Miura-Ko, B. Yolken, N. Bambos, and J. Mitchell, "Security investment games of interdependent organizations," in *Proceedings of 46th Annual Allerton Conference on Communication, Control, and Computing*, 2008, pp. 252–260.

[6] B. Johnson, J. Grossklags, N. Christin, and J. Chuang, "Are security experts useful? bayesian nash equilibria for network security games with limited information," in *European Symposium on Research in Computer Security*. Springer, 2010, pp. 588–606.

[7] B. Johnson, J. Grossklags, N. Christin, and J. Chuang, "Uncertainty in interdependent security games," in *International Conference on Decision and Game Theory for Security*. Springer, 2010, pp. 234–244.

[8] F. Farhadi, H. Tavafoghi, D. Teneketzis, and J. Golestani, "A dynamic incentive mechanism for security in networks of interdependent agents," in *Game Theory for Networks: 7th International EAI Conference, GameNets 2017 Knoxville, TN, USA, May 9, 2017, Proceedings*. Cham: Springer International Publishing, 2017, pp. 86–96.

[9] S. A. Hasheminasab and B. Tork Ladani, "Security investment in contagious networks," *Risk Analysis*, vol. 0, no. 0. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.12966

[10] M. Ezhei and B. Tork Ladani, "Interdependency analysis in security investment against strategic attacks," *Information Systems Frontiers*, Apr 2018. [Online]. Available: https://doi.org/10.1007/s10796-018-9845-8

[11] R. J. La, "Effects of degree correlations in interdependent security: Good or bad?" *IEEE/ACM Transactions on Networking*, vol. 25, no. 4, pp. 2484–2497, Aug 2017.

[12] A. Laszka and G. Schwartz, *Becoming Cybercriminals: Incentives in Networks with Interdependent Security*. Cham: Springer International Publishing, 2016, pp. 349–369.

[13] S. Shetty, M. McShane, L. Zhang, J. P. Kesan, C. A. Kamhoua, K. Kwiat, and L. L. Njilla, "Reducing informational disadvantages to improve cyber risk management†," *The Geneva Papers on Risk and Insurance - Issues and Practice*, Feb 2018. [Online]. Available: https://doi.org/10.1057/s41288-018-0078-3

[14] *DDoS attack that disrupted internet was largest of its kind in history, experts say*, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[15] M. Lelarge, "Coordination in network security games: a monotone comparative statics approach," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 11, pp. 2210–2219, 2012.

[16] X. Zhao, L. Xue, and A. B. Whinston, "Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements," *Journal of Management Information Systems*, vol. 30, no. 1, pp. 123–152, 2013. [Online]. Available: http://www.tandfonline.com/doi/abs/10.2753/MIS0742-1222300104

[17] R. J. La, "Interdependent security with strategic agents and cascades of infection," *IEEE/ACM Transactions on Networking*, vol. 24, no. 3, pp. 1378–1391, June 2016.

[18] F. Caccioli, M. Shrestha, C. Moore, and J. D. Farmer, "Stability analysis of financial contagion due to overlapping portfolios," *Journal of Banking & Finance*, vol. 46, pp. 233 – 245, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378426614001885

[19] K. G. Gkonis and H. N. Psaraftis, "Container transportation as an interdependent security problem," *Journal of Transportation Security*, vol. 3, no. 4, pp. 197–211, Dec 2010. [Online]. Available: https://doi.org/10.1007/s12198-010-0047-y

[20] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 42–49, January 2013.

[21] J. STRICKLAND, *10 Worst Computer Viruses of All Time*, https://computer.howstuffworks.com/worst-computer-viruses.htm/printable/.

[22] H. Ogut, S. Raghunathan, and N. Menon, "Citation for: Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of selfâĂŘprotection," *Risk Analysis*, vol. 31, no. 3, pp. 497–512. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6924.2010.01478.x

[23] D. T. Hoang, D. Niyato, and P. Wang, "Optimal cost-based cyber insurance policy management for mobile services," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Sept 2017, pp. 1–5.

[24] D. Niyato, D. T. Hoang, P. Wang, and Z. Han, "Cyber insurance for plug-in electric vehicle charging in vehicle-to-grid systems," *IEEE Network*, vol. 31, no. 2, pp. 38–46, March 2017.

[25] X. Lu, D. Niyato, N. Privault, H. Jiang, and P. Wang, "Managing physical layer security in wireless cellular networks: A cyber insurance approach," *IEEE Journal on Selected Areas in Communications*, pp. 1–1, 2018.

[26] A. Sarabi, P. Naghizadeh, Y. Liu, and M. Liu, "Risky business: Fine-grained data breach prediction using business profiles," *Journal of Cybersecurity*, vol. 2, no. 1, pp. 15–28, 2016. [Online]. Available: http://dx.doi.org/10.1093/cybsec/tyw004

[27] I. Vakilinia, S. J. louis, and S. Sengupta, "Evolving sharing strategies in cybersecurity information exchange framework," in *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, ser. GECCO '17. New York, NY, USA: ACM, 2017, pp. 309–310. [Online]. Available: http://doi.acm.org/10.1145/3067695.3075613

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

[29] I. Vakilinia, D. K. Tosh, and S. Sengupta, "Privacy-preserving cybersecurity information exchange mechanism," in *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, July 2017, pp. 1–7.

[30] I. Vakilinia, D. K. Tosh, and S. Sengupta, "Attribute based sharing in cybersecurity information exchange framework," in *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, July 2017, pp. 1–6.

[31] D. Kuru and S. Bayraktar, "The effect of cyber-risk insurance to social welfare," *Journal of Financial Crime*, vol. 24, no. 2, pp. 329–346, 2017.

[32] P. Naghizadeh and M. Liu, "Voluntary participation in cyber-insurance markets," in *Proceedings of the Workshop on the Economics of Information Security (WEIS)*, 2014.

[33] M. Lelarge and J. Bolot, "Economic incentives to increase security in the internet: The case for insurance," in *Proceedings of IEEE INFOCOM*, 2009, pp. 1494–1502.

[34] A. Hofmann, "Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks," *The Geneva Risk and Insurance Review*, vol. 32, no. 1, pp. 91–111, 2007.

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

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

[37] D. Woods, I. Agrafiotis, J. R. C. Nurse, and S. Creese, "Mapping the coverage of security controls in cyber insurance proposal forms," *Journal of Internet Services and Applications*, vol. 8, no. 1, p. 8, Jul 2017. [Online]. Available: https://doi.org/10.1186/s13174-017-0059-y

[38] 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, March 2017.

[39] 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, Sept 2018.

[40] M. M. Khalili, P. Naghizadeh, and M. Liu, "Embracing risk dependency in designing cyber-insurance contracts," in *Proceedings of 55th Annual Allerton Conference on Communication, Control, and Computing*, 2017.

[41] 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, April 2011.

[42] F. Massacci, J. Swierzbinski, and J. Williams, "Cyberinsurance and public policy: Self-protection and insurance with endogenous adversaries," 2017.

[43] 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*, vol. PP, no. 99, pp. 1–1, 2017.

[44] S. Evelsizer and B. Eaton, “Netdiligence 2016 cyber claims study,” 2016. [Online]. Available: https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf

[45] *Cybersecurity Professional Trends: A SANS Survey*, http://bit.ly/2rulxon.

APPENDIX

A.1. Proof of Theorem 2

Proof 2 (Theorem 2): Notice that $\overline{U}_o(f'_o) + \sum_{i=1}^{n} \overline{U}_i(f'_o) = \overline{V}_o(f'_o) + \sum_{i=1}^{n} \overline{V}_i(f'_o) = \overline{V}_{total}(f'_o)$. We assume that $\overline{U}_o(f^{\star}_o) \geq 0$, otherwise no insurer underwrites the SP. By the optimality of f^{**}_o for $\overline{V}_{total}(f'_o)$ we have,

$$\overline{V}_{max} = \overline{V}_{total}(f^{**}_o) \geq \overline{V}_{total}(f^{\star}_o) = \overline{U}_o(f^{\star}_o) + \sum_{i=1}^{n} \overline{U}_i(f^{\star}_o) \geq \sum_{i=1}^{n} \overline{U}_i(f^{\star}_o) = \overline{U}_{max} \tag{24}$$

Moreover, similar to the proof of theorem 1, by the first order condition we can show that,

$$f^{\star}_o = \left(f_o - (P'_o)^{-1}\left(\frac{b_o}{[l_o + q\cdot\sum_{i=1}^{n} l_i\cdot(t - t\cdot E(P_i(f_i)))]}\right)\right)^{+} \tag{25}$$

Also, from the proof of theorem 1, we have,

$$f^{**}_o = \left(f_o - (P'_o)^{-1}\left(\frac{b_o}{[l_o + \sum_{i=1}^{n} l_i\cdot(t - t\cdot E(P_i(f_i)))]}\right)\right)^{+} \tag{26}$$

Because $P_i^{'}(.)$ is an increasing function and $\frac{b_0}{[l_0 + q\cdot\sum_{i=1}^{n} l_i\cdot(t - t\cdot E(P_i(f_i)))]} > \frac{b_0}{[l_0 + \sum_{i=1}^{n} l_i\cdot(t - t\cdot E(P_i(f_i)))]}$, we have $f^{*}_o \leq f^{**}_o$.

A.2. Examples of the Loss Probability Function and Optimal Incentive Factors

Let's assume that $P_i(f_i) = \frac{q_i}{\frac{b_i\cdot(a_i - f_i)}{r_i} + 1}$, where q_i, a_i, r_i are constants and $q_i < 1$ and $a_i > f_{max}$. Then we have,

$$E\{P_i(f_i)\} = \frac{q_i\cdot r_i}{b_i\cdot(f_{max} - f_{min})} \ln \frac{b_i\cdot(a_i - f_{min}) + r_i}{b_i(a_i - f_{max}) + r_i} \tag{27}$$

Now we find f^{*}_o and f^{**}_o for the following examples,

- $P_o(f_o - f'_o) = \frac{p}{\frac{b_o\cdot(a - (f_o - f'_o))}{r} + 1}$, where p, a, r are constant.
  The optimal incentive factor f^{*}_o is given by,

$$f^{*}_o = (f_o - a + \frac{r}{b_o}(\sqrt{\frac{p\cdot l_o}{r}} - 1))^{+} \tag{28}$$

  Moreover, we can calculate f^{**}_o as follows,

$$f^{**}_o = (f_o - a + \frac{r}{b_o}(\sqrt{\frac{p\cdot[l_o + \sum_{i=1}^{n} l_i\cdot(t - t\cdot E(p_i(f_i)))]}{r}} - 1))^{+} \tag{29}$$

  Notice that $f^{**}_o \geq f^{*}_o$.
- $p_o(f_o - f'_o) = \frac{p}{(1 + \exp(\frac{b_o\cdot(a - (f_o - f'_o))}{r}))}$ where p, a, r are constants. Notice that this faction is not convex but we will show that $f^{**}_o \geq f^{*}_o$ in this case as well.
  The optimal incentive factor f^{*}_o is given by,
  - If $\frac{p\cdot l_o}{r} < 4$, then $f^{*}_o = 0$
  - If $\frac{p\cdot l_o}{r} > 4$ and $\frac{\frac{p\cdot l_o}{r} - 2 + \sqrt{(2 - \frac{p\cdot l_o}{r})^2 - 4}}{2} < \exp(\frac{b_o\cdot(a - f_o)}{r})$, then $f^{*}_o = 0$.

– Otherwise, f_o^* satisfies following equation:

$$\exp(\frac{b_o \cdot (a-(f_o-f_o^*))}{r}) = \frac{\frac{p \cdot l_o}{r} - 2 + \sqrt{(2-\frac{p \cdot l_o}{r})^2 - 4}}{2} \tag{30}$$

If the insurer underwrites the service provider and customers, then optimal incentive factor f_o^{**} is given by,

– If $\frac{p \cdot [l_o + \sum_{i=1}^n l_i \cdot (t - t \cdot E(P_i(f_i)))]}{r} < 4$, then $f_o^{**} = 0$

– If $\frac{p \cdot [l_o + \sum_{i=1}^n l_i \cdot (t - t \cdot E(P_i(f_i)))]}{r} > 4$ and $\frac{\frac{p \cdot \left[l_o + \sum_{i=1}^n l_i \cdot \left(t - t \cdot E(P_i(f_i))\right)\right]}{r} - 2 + \sqrt{(2 - \frac{p \cdot \left[l_o + \sum_{i=1}^n l_i \cdot \left(t - t \cdot E(P_i(f_i))\right)\right]}{r})^2 - 4}}{2} < \exp(\frac{b_o \cdot (a - f_o)}{r})$, then $f_o^{**} = 0$

– Otherwise, f_o^{**} satisfies following equation:

$$\exp(\frac{b_o \cdot (a-(f_o-f_o^{**}))}{r}) = \frac{\frac{p \cdot \left[l_o + \sum_{i=1}^n l_i \cdot \left(t - t \cdot E(P_i(f_i))\right)\right]}{r} - 2 + \sqrt{(2 - \frac{p \cdot \left[l_o + \sum_{i=1}^n l_i \cdot \left(t - t \cdot E(P_i(f_i))\right)\right]}{r})^2 - 4}}{2} \tag{31}$$

Because $[l_o + \sum_{i=1}^n l_i \cdot (t - t \cdot E(P_i(f_i)))] \geq l_o$, then $f_o^{**} \geq f_o^*$ in this case as well.

- $p_o(f_o - f_o') = q + p \exp(-\frac{b_o \cdot (a-(f_o-f_o'))}{r})$, where p, q, r, a are constant and $p + q < 1$ and $f_o < a$. By the first order condition we have,

$$f_o^* = \left(f_o - a - \frac{r}{b_o} \ln \frac{r}{p \cdot l_o}\right)^+ \tag{32}$$

Moreover, f_o^{**} is given by,

$$f_o^{**} = \left(f_o - a - \frac{r}{b_o} \ln \frac{r}{p \cdot [l_o + \sum_{i=1}^n l_i \cdot (t - t \cdot E(P_i(f_i)))]}\right)^+ \tag{33}$$

All of the above examples imply that the insurer should offer higher discount factor when she underwrites the SP and the customers as compared to the optimal incentive factor which maximizes $\overline{V}_o(f_o')$.

A.3. Cyber-insurance policy: CyberSecurity by Chubb

Premium Calculation

Premiums are calculated by size and type-of-operation, and coverage characteristics associated with e-risks. The policy premium is the sum of the Cyber Liability premium (Coverage A); the premium for any selected optional coverage grants (Coverages B through H); and the premium for the Premier Privacy rate bearing endorsement, if selected.

The limit for any selected optional coverage grant may vary from the Cyber Liability coverage limit, but must be less than or equal to the Cyber Liability coverage limit. Similarly, the retention for any selected optional coverage grant may vary from the Cyber Liability coverage retention (without further restriction).

The Cyber Liability premium is calculated as follows:

(Section 1 Base Rate) x (Section 2 Industry Factor) x (Section 3.1 ILF) x (Section 3.2 Retention Factor) x (Section 3.3 Coinsurance Factor) x (Section 6 Third-Party Modifier Factors)

The premium for optional coverage grants B and C1 are calculated as follows:

(Section 1 Base Rate) x (Section 2 Industry Factor) x (Section 3.3 Coinsurance Factor) x (Section 4.#.I Base Rate Factor) x (Section 4.#.II ILF) x (Section 4.#.III Retention Factor) x (Section 6 Third-Party Modifier Factors) *where # corresponds to the respective coverage grant letter*

The premium for optional coverage grant C2 (Re d Expenses) is calculated as follows:

(Section 2 Industry Factor) x (Section 3.3 Coinsurance Factor) x (Section 4.C2 Base Premium) x (Section 6 Third-Party Modifier Factors)

The premium for optional coverage grants D, E, F, G and H are calculated as follows:

(Section 1 Base Rate) x (Section 2 Industry Factor) x (Section 3.3 Coinsurance Factor) x (Section 4.#.I Base Rate Factor) x (Section 4.#.II ILF) x (Section 4.#.III Retention Factor) x (Section 7 First-Party Modifier Factors) *where # corresponds to the respective coverage grant letter*

The premium for the Premier Privacy endorsement is calculated as follows:

(Section 1 Base Rate) x (Section 2 Industry Factor) x (Section 3.1 ILF) x (Section 3.2 Retention Factor) x (Section 3.3 Coinsurance Factor) x (Section 5 Premier Privacy Endorsement Factor) x (Section 6 Third-Party Modifier Factors)

Section 2: Industry Factors: The appropriate factor should be applied multiplicatively.

Industry – Non-Financials	Factor
Accounting Firms	0.85
Advertising Firms	0.85
Agriculture	0.85
Construction	0.85
Consulting Firms	0.85
Entertainment Industry (PCI* Level 3 – 4)	0.85
Hospitality Industry (PCI* Level 3 – 4)	0.85
Human Resources Firms	0.85
Law Firms	0.85
Manufacturing	0.85
Media Firms	0.85
Other Professional Services Firms	0.85
Publishing Firms	0.85
Retail Merchants; such as Clothing, Grocery (PCI* Level 3 – 4)	0.85
Technology Developers (Software and Hardware Providers)	0.85
Transportation Companies	0.85
All Other Non-Financials	1.00
Energy; such as Oil & Gas, Natural Resources (excluding Utilities)	1.00
Entertainment Industry (PCI* Level 1 – 2)	1.00
Hospitality Industry (PCI* Level 1 – 2)	1.00
Labor Management Trusts	1.00
Not-for-Profit Organizations	1.00
Unions	1.00
Bio-Technology / Pharmaceutical	1.20
Data Aggregators	1.20
Educational Institutions (Schools, Colleges, Universities)	1.20
Gaming (including Online)	1.20
Government Agencies	1.20
Medical / Healthcare Related Services	1.20
Municipalities (Local, County, State)	1.20
Payroll Processing	1.20
Retail Merchants (PCI* Level 1 – 2)	1.20
Technology Service Providers (ASP, Portals, Web Search Engines)	1.20
Telecommunications (including Cable, Internet Service Providers)	1.20
Utilities	1.20

*PCI: Payment Card Industry Data Security Standards

Section 3: Increased Limit Factors, Retention Factors and Coinsurance Factors

1. **Increased Limit Factors:** The appropriate factor should be applied multiplicatively.

   a. For a limit ≤ $1 million the factors in the chart below apply.

Limit	Factor
$100,000	0.300
$250,000	0.500
$500,000	0.700
$1,000,000	**1.000**

   Linear interpolation should be used to determine an Increased Limit Factor (ILF) if the desired limit is not shown above (rounded to 3 decimal places).

   b. For a limit > $1 million the ILF is calculated using the following exponential formula (rounded to 3 decimal places): ILF = (limit ÷ 1,000,000)^0.68

   The table below show sample ILFs calculated using the above formula:

Limit	Factor
$1,000,000	1.000
$2,000,000	1.602
$2,500,000	1.865
$3,000,000	2.111
$4,000,000	2.567
$5,000,000	2.987
$7,500,000	3.936
$10,000,000	4.786
$15,000,000	6.306
$20,000,000	7.668
$25,000,000	8.925

Section 4: Optional Coverage Grants

The following coverage grants are available for an additional premium. The limits selected for each of coverage grants B through H can vary from the limit selected in Section 3.1 for Coverage A, but must be less than or equal to the limit selected for Coverage A. The retentions selected for each of coverage grants B through H can vary from the retention selected in Section 3.2 for Coverage A.

B. Privacy Notification Expenses:

I. Base Rate Factors
Base rate factors are for a $1 million limit of liability and a base retention as determined in Section 1. The appropriate base rate factor should be applied multiplicatively.

Privacy Notification Expenses Factor: 0.15

II. Increased Limit Factors
Select a limit for Coverage B less than or equal to the limit selected for Coverage A. Calculate the ILF using the applicable rules and table/formula of Section 3.1.

III. Retention Factors
Select a retention for Coverage B. Calculate the Retention Factor using the applicable rules and table of Section 3.2.

C1. Crisis Management Expenses:

I. Base Rate Factors
Base rate factors are for a $1 million limit of liability and a base retention as determined in Section 1. The appropriate base rate factor should be applied multiplicatively.

Crisis Management Expenses Factor: 0.02

II. Increased Limit Factors
Select a limit for Coverage C1 less than or equal to the limit selected for Coverage A. Calculate the ILF using the applicable rules and table/formula of Section 3.1.

III. Retention Factors
Select a retention for Coverage C1. Calculate the Retention Factor using the applicable rules and table of Section 3.2.

E. E-Theft Loss:

I. Base Rate Factors

Base rate factors are for a $1 million limit of liability and a base retention as determined in Section 1. The appropriate base rate factor should be applied multiplicatively.

E-Theft Loss Factor: 0.25

II. Increased Limit Factors

Select a limit for Coverage E less than or equal to the limit selected for Coverage A. Calculate the ILF using the applicable rules and table/formula of Section 3.1.

III. Retention Factors

Select a retention for Coverage E. Calculate the Retention Factor using the applicable rules and table of Section 3.2.

F. E-Communicaton Loss:

I. Base Rate Factors

Base rate factors are for a $1 million limit of liability and a base retention as determined in Section 1. The appropriate base rate factor should be applied multiplicatively.

E-Communication Loss Factor: 0.10

II. Increased Limit Factors

Select a limit for Coverage F less than or equal to the limit selected for Coverage A. Calculate the ILF using the applicable rules and table/formula of Section 3.1.

III. Retention Factors

Select a retention for Coverage F. Calculate the Retention Factor using the applicable rules and table of Section 3.2.