

Competitive Cyber-Insurance and Internet Security

Nikhil Shetty, Galina Schwartz, Mark Felegyhazi, and Jean Walrand

Abstract This paper investigates how competitive cyber-insurers affect network security and welfare of the networked society. In our model, a user's probability to incur damage (from being attacked) depends on both his security and the network security, with the latter taken by individual users as given. First, we consider cyber-insurers who cannot observe (and thus, affect) individual user security. This asymmetric information causes moral hazard. Then, for most parameters, no equilibrium exists: *the insurance market is missing*. Even if an equilibrium exists, the insurance contract covers only a minor fraction of the damage; network security worsens relative to the no-insurance equilibrium. Second, we consider insurers with perfect information about their users' security. Here, user security is perfectly enforceable (zero cost); each insurance contract stipulates the required user security. The unique equilibrium contract covers the entire user damage. Still, for most parameters, network security worsens relative to the no-insurance equilibrium. Although cyber-insurance improves user welfare, in general, competitive cyber-insurers fail to improve network security.

Nikhil Shetty
UC Berkeley, Berkeley-94720, e-mail: nikhils@eecs.berkeley.edu

Galina Schwartz
UC Berkeley, Berkeley-94720, e-mail: schwartz@eecs.berkeley.edu

Mark Felegyhazi
ICSI, Berkeley-94704, e-mail: mark@icsi.berkeley.edu

Jean Walrand
UC Berkeley, Berkeley-94720, e-mail: wlr@eecs.berkeley.edu

1 Introduction

In this paper,¹ we propose a model to study the effects of cyber insurance on user security and their welfare. Our model highlights how network externalities combined with information asymmetry lead to a *missing market for cyber insurance*.

The Internet serves as a ubiquitous communication platform for both individuals and businesses. Thus, an increasing amount of wealth is accessible online, and cyber-crime is becoming one of the most lucrative criminal activities. Cyber-crime is lucrative because network vulnerabilities are easy to exploit and persecution of cyber-criminals is plagued by enforcement problems. First, and importantly, criminals are relying on the anonymity of the Internet protocols to disguise their traces. Second, global Internet connectivity makes it difficult for law enforcement authorities to identify the origin of the attacks. Exploiting national differences in legal systems, criminals often operate safely from countries with the weakest legislations and enforcement. Third, criminals quickly adapt their attack strategies as new defenses are developed; thus, cyber-crime evolves to minimize the chance of persecution. Altogether, this situation results in formation of highly professional, mafia-style cyber-crime establishments, which are rapidly expanding, see [2].

Technology-based defense and enforcement solutions are available, but there is a consensus among security researchers [2] that the existing security problems cannot be solved by technological means alone. We concur that these security problems primarily result from misaligned incentives of the networked parties with respect to their security. Existing research [4, 7, 16, 19, 18] indicates that *risk management* in general and cyber-insurance in particular are potentially valuable tools for security management. Still, at present, risk management capabilities are virtually nonexistent in the network [2].

We model the effects of informational asymmetries in the presence of network externalities, and study their consequences for network security incentives. We believe that these features of the environment induce socially suboptimal network security, and complicate the management of security risks. We build on the seminal ideas of Akerlof [1], Rothschild and Stiglitz [17] and others,² which we combine with the ideas of interdependent security originated by Heal-Kunreuther [14], Gordon-Loeb [8] and Hausken [11].³

In our model, all users are identical, meaning that their wealth is identical and they suffer identical damage if successfully attacked. The user's probability of being attacked depends on both the *user security level* and the *network security level*, which individual users take as given. Thus, we have an externality. Indeed, due to this externality, individually optimal user security level is lower than the socially optimal one.

¹ This work was funded in part by the National Science Foundation under grant NSF-0433702. Any opinions, findings, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding source.

² See [20] for the literature review.

³ See also [7, 9, 21, 5, 10, 3, 6, 13, 12]. This list is by no means exhaustive.

Our setting emphasizes that interdependent security is a focal feature, which shapes the incentives for Internet security. Although security interdependence is present in other contexts (such as terrorist attacks [15]), network security is especially prone to these effects because everyone is interlinked.

First, we investigate the effects of information asymmetry in the presence of network effects. Though our model allows to study both moral hazard (when insurers are not aware of user security levels) and adverse selection (when insurers cannot distinguish different user types), in this paper, we address only moral hazard. We demonstrate that for a wide range of parameters, insurance market fails to exist, i.e., we observe a *missing market*.

Next, we assume no information asymmetry between the insurers and the insured (users). We demonstrate that user utility is higher with insurance, but the network security level is not necessarily higher. On reverse, in many cases network security worsens with insurers. Indeed, insurers only *manage* risks, but they do not necessarily reduce them.

Our homogeneity assumption is simplistic, and does not hold in the actual Internet. But, adding user and insurer heterogeneity to our setting only adds more informational asymmetries. Then, the lemon problem becomes likely, which itself could cause missing markets [1]. Thus, with heterogeneity, one expects adverse selection problems, which would also contribute to missing markets.

We make two main contributions to the literature. First, we observe that even with no heterogeneity (of users and insurers), information asymmetries complicate the formation of viable cyber-insurance markets. Second, we demonstrate that even in the absence of informational asymmetries, competitive cyber-insurers fail to improve network security. The significant implication is that in the existing network environment, cyber-insurance markets cannot serve as a catalyst for improvement of network security.

The paper is organized as follows. In Section 2, we propose a base model, derive its Nash equilibrium, and compare it with socially optimal allocation. In Section 3, we add competitive insurers to our base model, analyze the equilibrium with insurers. We consider two cases: when individual security levels are non-contractible and when insurers include the requirement about individual security level into the contract. In Section 4, we summarize our findings and conclude. The technical details are relegated to Appendix.

2 Model

In this section, we present our base model, which highlights the interdependence of user and network security. We consider a network populated by identical users. Each user i has two choice variables: the *convenience* level $a_i > 0$ of his network activity, and his *security* level $s_i \in [0, 1]$. The *convenience* level a_i can be, for example, characterized by the number of applications utilized by the user, such as emails, Web, IM, P2P, etc. If there are no security problems, the user derives utility from

his wealth and from network usage. We assume that both these components of user utility U_i are additively separable:

$$U_i = K_1 \cdot f(W) + K_2 \cdot g(a_i) - K_3 \cdot a_i,$$

where K_1 , K_2 and K_3 are positive constants, and $W > 0$ denotes user's wealth. We assume that the functions f and g are increasing and concave, reflecting that user wealth W and *convenience* level a_i have a positive but decreasing marginal benefit for the user. To increase his *convenience* level, user incurs a linear cost (cost of effort).

In the presence of network attacks, we assume that, if the attack on the user is successful, the user incurs a monetary damage $D \in (0, W)$. Let p_i be the probability that user i suffers such an attack. This probability depends on two factors: the network security level $\bar{s} \in [0, 1]$, which determines the probability of a user being attacked, and the user security level s_i , which determines the probability of success of such an attack. This justifies our expression for p_i :

$$p_i = (1 - s_i) \cdot (1 - \bar{s}) = v_i \cdot \bar{v}, \quad (1)$$

where for mathematical convenience, we introduce the *user vulnerability* level $v_i = 1 - s_i$ and the *network vulnerability* level $\bar{v} = 1 - \bar{s}$. Further, assume that \bar{s} is equal to the average security levels of its users:

$$\bar{s} = \frac{\sum_{i=1, \dots, N} s_i}{N}, \quad (2)$$

and we let the number of users N be large enough so that a single user has a negligible effect on the network security level. Thus, each user takes the network security level as a given parameter.

We assume that user's choice of a higher security requires a higher user cost (in terms of effort), and this cost is proportional to the convenience level. Again, assuming additive separability, we express the expected utility of user i in the presence of network insecurity as:

$$E[U_i] = K_1 \{(1 - p_i) \cdot f(W) + p_i \cdot f(W - D)\} + K_2 \cdot g(a_i) - K_3 \cdot a_i \cdot (h(s_i) + 1), \quad (3)$$

where the security cost function, $h(\cdot)$ is increasing and convex ($h', h'' > 0$) with $h(0) = 0$ corresponding to zero security level and $h(1) = \infty$, corresponding to a hypothetical "perfectly secure" system. Thus, it becomes increasingly costly to improve the security level at a higher level of security.

For simplicity, we let $f(x) = g(x) = \sqrt{x}$ and $h(x) = \frac{1}{\sqrt{1-x}} - 1$ and solve the problem for these specific functions. Then, (3) becomes:

$$E[U_i] = K_1 \left\{ (1 - p_i) \sqrt{W} + p_i \sqrt{W - D} \right\} + K_2 \sqrt{a_i} - K_3 a_i \frac{1}{\sqrt{v_i}}. \quad (4)$$

Since we assume that the convenience level of user i 's network usage a_i is not affected even when this user is attacked, this model may be more suitable for attacks like phishing, eavesdropping, etc. rather than for attacks like denial-of-service.

2.1 Analysis

We start by deriving the optimal convenience level a_i^* by taking the partial derivative of (4) with respect to a_i :

$$\frac{\partial E[U_i]}{\partial a_i} = K_2 \frac{1}{2} \frac{1}{\sqrt{a_i}} - K_3 \frac{1}{\sqrt{v_i}},$$

from which a_i^* is:

$$a_i^* = \frac{1}{4} \frac{K_2^2}{K_3^2} v_i. \quad (5)$$

Thus, the user's a_i^* depends only on her choice of v_i , but not on network vulnerability level \bar{v} . Next, we substitute (5) in (4) to obtain:

$$E[U_i] = \frac{1}{4} \frac{K_2^2}{K_3^2} [\sqrt{v_i} - v_i \bar{v} K (\sqrt{W} - \sqrt{W-D}) + K \sqrt{W}] \quad (6)$$

where $K = \frac{4K_1K_3}{K_2^2}$. To simplify, we let $\frac{1}{4} \frac{K_2^2}{K_3^2} = 1$, and obtain a normalized utility:

$$E[U_i] = \sqrt{v_i} - v_i \bar{v} K (\sqrt{W} - \sqrt{W-D}) + K \sqrt{W}. \quad (7)$$

The constant K characterizes how users value their wealth relative to the utility from the network.

2.1.1 Nash Equilibrium

To find the user i 's best response $v_i^*(\bar{v})$ to a given network vulnerability \bar{v} , we optimize (7) with respect to v_i (subject to $v_i \leq 1$) and express $v_i^*(\bar{v})$ as

$$v_i^*(\bar{v}) = \min \left\{ \frac{1}{[2\bar{v}K(\sqrt{W} - \sqrt{W-D})]^2}, 1 \right\}. \quad (8)$$

From (8), $v_i^*(\bar{v})$ is identical for all users, from which any Nash equilibrium is symmetric, and let $v_i^*(\bar{v}) = v_j^*(\bar{v}) = v^*$ for any users i and j . Then, from (2), we have $\bar{v} = v^*$ and hence,

$$v^* = \min \left\{ \frac{1}{[2v^*K(\sqrt{W} - \sqrt{W-D})]^2}, 1 \right\},$$

from which we obtain Nash equilibrium vulnerability v^* :

$$v^* = 1 - s^* = \min \left\{ \frac{1}{[2K(\sqrt{W} - \sqrt{W-D})]^{2/3}}, 1 \right\}. \quad (9)$$

From (9), $v^* < 1$ only if $\sqrt{W} - \sqrt{W-D} > \frac{1}{2K}$ and thus, all else equal, users invest in security only when their damage D or K become sufficiently high, or when user wealth W is low.

2.1.2 Social Optimum

We assume that a social planner unilaterally dictates user vulnerability, $v_i = v$, and maximizes cumulative utility of the users. Since users are identical, this maximization is identical to a representative user utility maximization with $\bar{v} = v$. From (7), the representative user utility is:

$$E[U] = \sqrt{\bar{v}} - v^2 K(\sqrt{W} - \sqrt{W-D}) + K\sqrt{W}. \quad (10)$$

Maximizing (10), subject to $v \leq 1$, we obtain the socially optimal vulnerability v^{soc} as:

$$v^{soc} = 1 - s^{soc} = \min \left\{ \frac{1}{[4K(\sqrt{W} - \sqrt{W-D})]^{2/3}}, 1 \right\}. \quad (11)$$

Thus, $v^{soc} < 1$ only if $(\sqrt{W} - \sqrt{W-D}) > \frac{1}{4K}$. As expected, $v^{soc} \leq v^*$, which allows us to formulate the following proposition:

Proposition 1. *When the socially optimal security level is strictly positive, it is strictly higher than the individually optimal one: $s^{soc} > s^*$. Users are strictly better off in the social optimum than in the Nash equilibrium.*

In the next section, we extend this model to the presence of competitive insurers. We will investigate how insurer information about user security level (or lack of such information) impacts network security.

3 Insurance Model

We define market equilibrium similar to the model of Rothschild and Stiglitz [17], who pioneered the examination of equilibria in insurance markets with information asymmetries. We assume that each insurer offers a single insurance contract in a *class of admissible contracts*, or does nothing. A Nash equilibrium is defined as a set of admissible contracts such that: i) all contracts result in a non-negative utility for the insurers, ii) taking as given the contracts offered by incumbent insurers (those offering contracts), there is no additional contract which an entrant-insurer (one not offering a contract) can offer and make a strictly positive profit and iii) taking as

given the set of contracts offered by other incumbent insurers, no incumbent can increase its profits by altering his offered contract. The literature referred to such contracts as “competitive”, because entry and exit are free, and because no barrier to entry or scale economies are present.

We consider risk neutral insurers who compete with each other. Let ρ be the premium charged to a user and $L > 0$ be his loss covered by the insurer. We do not consider $L < 0$ because it is unrealistic to expect a fine when a user suffers a damage. Let v and \bar{v} be the user and network vulnerability. Then, we denote the respective user utility by $U(v, \bar{v}, \rho, L)$, and from (7) and (1), we have:

$$U(v, \bar{v}, \rho, L) = \sqrt{\bar{v}} + v\bar{v}K\sqrt{W - D + L - \rho} + (1 - v\bar{v})K\sqrt{W - \rho}. \quad (12)$$

If v, ρ, L are identical for all users, then $v = \bar{v}$, and we obtain

$$U(v, v, \rho, L) = \sqrt{v} + v^2K\sqrt{W - D + L - \rho} + (1 - v^2)K\sqrt{W - \rho}. \quad (13)$$

Additionally, we will assume that insurers take network security \bar{v} as given. This assumption reflects that individual insurers cannot affect \bar{v} on their own.

3.1 Insurance with Non-Contractible Security

In this section, we assume that it is impossible (or too costly) for the insurers to monitor the users’ security level. Indeed, even if v is included in the contract and user compliance is observable by the insurer, but unverifiable in court (due to the prohibitively high costs), the insurer would effectively operate as if no requirement on v is imposed. Thus, we consider the contracts of the form (ρ, L) only. In addition, we will assume that contracts stipulate that purchase of extra coverage from outside parties is prohibited. Further, since the users are homogeneous, we will restrict our attention to a symmetric equilibrium, i.e., the equilibria with identical user actions. Henceforth, we will use the superscript \ddagger to distinguish the values in such an equilibrium.

Let user i purchase a contract (ρ, L) . Then, he will choose his vulnerability v_i to maximize his utility (taking \bar{v} as given):

$$E[U_i] = \sqrt{v_i} - v_i\bar{v}K(\sqrt{W - \rho} - \sqrt{W - D + L - \rho}) + K\sqrt{W - \rho}. \quad (14)$$

Any contract which improves user utility $U(v, \bar{v}, \rho, L)$ is preferred by users to any other contract. Hence, in equilibrium, there should exist no such deviating contract that makes non-negative profits for an insurer. Further, the equilibrium contract is constrained by user participation - a user must prefer to buy insurance, assuming that others already did so, to staying without insurance. In Appendix, we show that this participation constraint never binds, and, in equilibrium, due to competition, insurers’ profits are zero: $\rho^\ddagger = (v^\ddagger)^2 L^\ddagger$. Further, we demonstrate that, in any equilibrium:

$$L^\ddagger < D,$$

and from user optimization, we have:

$$v^\ddagger = \frac{1}{\left[2K(\sqrt{W - \rho^\ddagger} - \sqrt{W - D} + (L^\ddagger - \rho^\ddagger))\right]^{2/3}}. \quad (15)$$

Comparing (15) with (9), we infer that in any equilibrium:

$$v^\ddagger > v^*. \quad (16)$$

Although the availability of insurance may allow users to reach a higher utility, the network security is strictly lower with insurance. In Appendix, we prove the following proposition:

Proposition 2. *If $D < \frac{8}{9}W$, any insurance contract with security levels unobservable by the insurers strictly decreases the utility of the users. Hence, no insurance is offered and no insurance market exists. If $D > \frac{8}{9}W$, there could exist an equilibrium in which all users purchase insurance contract $(\rho^\ddagger, L^\ddagger)$. This insurance improves users' utility relative to the no insurance case, but decreases their security (i.e., $v^\ddagger > v^*$ is always true).*

From Proposition 2, the presence of insurers negatively affects network security. Indeed, here, security is chosen by the users, and insured users have meager incentives to secure themselves. This is a typical manifestation of a moral hazard. In this case, the expected per user loss due to network insecurity increases by:

$$\Delta^\ddagger = [(v^\ddagger)^2 - (v^*)^2] D.$$

3.2 Insurance with Contractible Security

In this section, we assume that insurers can enforce a desired security level for the insured users at zero cost. Thus, we permit contracts (v, ρ, L) to specify a user's required vulnerability v . In reality, this may be achieved, for example, by deploying tamper-proof security software that monitors and enforces user security.

3.2.1 Social Planner

Next, we derive the social planner choice of contract when security is contractible. Let $(v^\ddagger, \rho^\ddagger, L^\ddagger)^{soc}$ be the contract chosen by a social planner. The social planner objective is to maximize the user utility, subject to the constraint of non-negative profits:

$$\begin{aligned} & \max_{\rho, v, L} U(v, v, \rho, L) \\ & \text{s.t.} \quad v^2 L \leq \rho \text{ and } v \leq 1. \end{aligned}$$

In Appendix, we solve this optimization problem, and derive the following social planner's equilibrium:

$$\rho^{\dagger soc} = (v^{\dagger soc})^2 L^{\dagger soc},$$

and full coverage will be offered since users prefer it:

$$L^{\dagger soc} = D.$$

If the equilibrium vulnerability $v^{\dagger soc} < 1$, then it must be a solution of:

$$\frac{v^3}{W - v^2 D} = \frac{1}{(2KD)^2}, \quad (17)$$

which we have proven to be unique.

3.2.2 Competitive Insurers

Any insurance contract (v, ρ, L) that achieves a higher user utility $U(v, \bar{v}, \rho, L)$ would be preferred to other contracts. In equilibrium, there should exist no contract that permits non-negative insurer profits and yields a higher user utility than the equilibrium contract does. In addition, we modify the definition of insurance market equilibrium in Section 3 and assume that no single insurer affects the network vulnerability. This assumption is realistic since competitive insurers lack market power. The participation constraint must hold in equilibrium, i.e., insured users must obtain at least the same utility with insurance than by staying uninsured. In Appendix, we show that only a unique contract can exist in equilibrium. Let this equilibrium contract be denoted by $(v^\dagger, \rho^\dagger, L^\dagger)$.

In Appendix, we demonstrate that, in equilibrium, insurers make zero profits and offer full coverage since users prefer it.

$$\rho^\dagger = (v^\dagger)^2 L^\dagger, \text{ and } L^\dagger = D.$$

If the equilibrium vulnerability $v^\dagger < 1$, then it must be a solution of:

$$\frac{v^3}{W - v^2 D} = \frac{1}{(KD)^2}, \quad (18)$$

which we have proven to be unique. From (17) and (18), we conclude that the vulnerability in the competitive insurer equilibrium is higher than that in the social optimum: $v^\dagger > v^{\dagger soc}$. In Appendix, we also derive the condition for $v^\dagger < v^*$. We find that equilibrium vulnerability only improves (relative to the Nash equilibrium without insurance) when $\frac{D}{W}$ is lower than some critical value. This critical value is achieved only when v^* is close to 1, i.e., when user security is close to zero in the

no-insurance Nash equilibrium. Thus, for a large range of parameters, $v^\dagger > v^*$, i.e., the presence of insurance leads to a higher vulnerability.

This permits us to formulate the following proposition:

Proposition 3. *With insurers present, and security levels contractible, in any equilibrium, full coverage $L^\dagger = D$ is offered. For most parameters, equilibrium network security is lower than in the no-insurance equilibrium. Only when user security is low in the no-insurance Nash equilibrium (i.e., v^* close to 1), the presence of insurers improves network security.*

From Proposition 3, with security levels observable by the insurers, the insurers' presence allows to improve user welfare, but hardly improves network security. When $v^\dagger < v^*$, the insurers' presence reduces the per user expected loss from network insecurity by Δ^\dagger , where:

$$\Delta^\dagger = [(v^*)^2 - (v^\dagger)^2] D.$$

Else, the per user expected loss increases by

$$\Delta^\dagger = [(v^\dagger)^2 - (v^*)^2] D.$$

Figure 1(a) depicts the equilibrium security level of users (and hence the network security level) as a function of the damage D while Figure 1(b) depicts the equilibrium utility of users as a function of D . The parameter values used are $K = 1$ and $W = 100$.

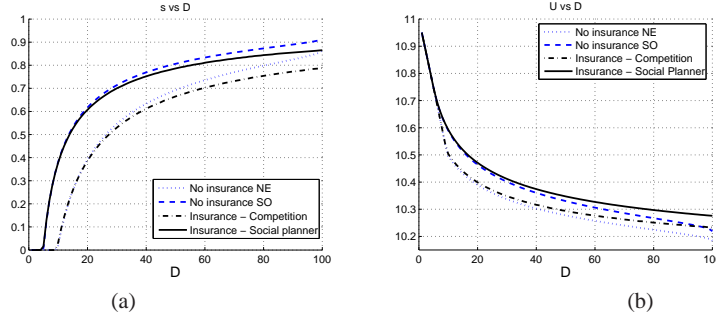


Fig. 1 (a) Security level and (b) utility of homogeneous users in equilibrium as a function of the damage $0 < D < W$. Here $W = 1000$ and $K = 1$.

4 Conclusion

In this paper, we investigate the effects of competitive cyber-insurers on network security and welfare. We highlight the impact of asymmetric information in the presence of network externalities and address the effects of interdependent security on the market for cyber-risks. The existing literature attributes cyber-insurance a significant role in cyber-risk management; it especially emphasizes positive effects of cyber-insurance market on security incentives. We find that, on reverse, the presence of competitive cyber-insurers weakens user incentives to improve security.

First, we consider insurers who cannot observe (and thus, cannot contract) user security; here, insurers observe the network security only. Then, the moral hazard problem is present, i.e., with more insurance coverage, the users' incentives to invest in security become meager. In this case, for most parameters, the insurance market collapses, i.e., no insurance is offered in equilibrium. Even if cyber-insurance exists, it covers a minor fraction of damages only. Our findings are in line with the existing Internet, where cyber-insurance is scantily observed.

Second, we consider insurers who observe (and thus, can contract) user security. Here, insurers' contracts include user security level which insurers enforce at zero cost, and thus, no moral hazard is present. Still, in general, competitive insurers fail to improve upon the security level of the no-insurance equilibrium. Though insurance improves the utility for risk-averse users, it does not serve as an incentive device for improving security practices. Indeed, insurance is a tool for risk management and redistribution, not necessarily a tool for risk reduction.

To sum up, we argue that a combination of network effects and information asymmetries leads to difficulties in formation of viable insurance markets for cyber risks. Thus, our results dash the hopes for both, expectations of development of cyber insurance markets under the current network environment, and for the beliefs that such markets may serve as a catalyst for improvement of network security.

5 Appendix

Proof of Proposition 2

When the user vulnerability v is non-contractible, the contracts have the form (ρ, L) , and v is selfishly chosen by the users. Since our users are homogeneous, we will restrict our attention to a symmetric equilibrium, i.e., user actions in equilibrium are identical. Let $(\rho^\diamond, L^\diamond)$ be such an equilibrium insurance contract and \bar{v}^\diamond be the resulting network vulnerability. First, we show that in any equilibrium $L^\diamond < D$.

Assume the reverse and let $(\rho^\diamond, L^\diamond = D)$ be an equilibrium. In this case, it is optimal for each user to choose $v = 1$. Hence, $\bar{v}^\diamond = 1$ and $\rho^\diamond = D$ for non-negative insurer profits. From (13), $U(1, 1, D, D) = U(1, 1, 0, 0)$, which implies that the user is indifferent between buying and not buying insurance. If the vulnerability in the no-insurance Nash equilibrium $v^* < 1$, then the user's participation constraint does

not hold: $U(v_i, 1, 0, 0) > U(1, 1, D, D)$ for some $v_i < 1$. This is a contradiction since user i is better off not purchasing such an insurance, and therefore $L^\diamond < D$.

To determine the vulnerability that the insured user chooses selfishly, we differentiate his utility with respect to v , keeping \bar{v} fixed:

$$\frac{\partial U(v, \bar{v}^\diamond, \rho^\diamond, L^\diamond)}{\partial v} = 0,$$

and we have

$$v = \frac{1}{(2\bar{v}^\diamond K(\sqrt{W - \rho} - \sqrt{W^D + L - \rho}))^2}. \quad (19)$$

where $W^D = W - D$. In equilibrium, $v = \bar{v}^\diamond$ and from (19), we obtain (similar to (9)):

$$\bar{v}^\diamond = \frac{1}{[2K(\sqrt{W - \rho^\diamond} - \sqrt{W^D + (L^\diamond - \rho^\diamond)})]^{2/3}}, \quad (20)$$

Comparing (20) with (9), we infer that:

$$v^* < \bar{v}^\diamond, \quad (21)$$

because

$$\sqrt{W - \rho^\diamond} < \sqrt{W} \text{ and } \sqrt{W^D + (L^\diamond - \rho^\diamond)} \geq \sqrt{W^D}.$$

Next, let us make sure that no user deviates and stays without insurance, that is the participation constraint holds. For the uninsured user i , utility is maximized at

$$v_i = \frac{1}{(\bar{v}^\diamond)^2 [2K(\sqrt{W} - \sqrt{W^D})]^2}. \quad (22)$$

Comparing this with (9), we have

$$v_i (\bar{v}^\diamond)^2 = (v^*)^3,$$

and from (21),

$$v_i = \left(\frac{v^*}{\bar{v}^\diamond}\right)^2 v^* < v^*,$$

and his maximum attainable utility is

$$\begin{aligned} U_i &= \sqrt{v_i} + v_i \bar{v}^\diamond [2K(\sqrt{W} - \sqrt{W^D})] + K\sqrt{W} \\ &= \left(\frac{v^*}{\bar{v}^\diamond}\right) \sqrt{v^*} + \left(\frac{v^*}{\bar{v}^\diamond}\right) (v^*)^2 [2K(\sqrt{W} - \sqrt{W^D})] + K\sqrt{W} < U^*. \end{aligned} \quad (23)$$

Note that $U^* = U(v^*, v^*, 0, 0)$. Hence, for $(\rho^\diamond, L^\diamond)$ to be an equilibrium contract, $U(v^\diamond, \bar{v}^\diamond, \rho^\diamond, L^\diamond) > U(v^*, v^*, 0, 0) = U^*$. Then, from (23),

$$U_i < U^* < U(v^\diamond, \bar{v}^\diamond, \rho^\diamond, L^\diamond),$$

and we infer that the participation constraint does not bind.

Next, we show that, if $D < \frac{8}{9}W$, the only equilibrium contract is $(0, 0)$. Consider a contract (ρ, L) and let \tilde{v} be the vulnerability obtained from (20). Due to insurer competition, in any equilibrium

$$\rho = \tilde{v}^2 L. \quad (24)$$

If not, an entrant insurer could design another contract that yields lower profits, which users prefer since it maximizes their utility. The user utility is obtained by substituting (20) in (12). Then, we have

$$U = K\sqrt{W - \rho} + \frac{1}{(16K(\sqrt{W - \rho} - \sqrt{W^D + L - \rho}))^{1/3}}. \quad (25)$$

Using (24), we rewrite (25) as $K\sqrt{W - \tilde{v}^2 L} + \frac{1}{(16K(\sqrt{W - \tilde{v}^2 L} - \sqrt{W^D + L - \tilde{v}^2 L}))^{1/3}}$.

Let $\dot{\tilde{v}}$ denote $\frac{\partial \tilde{v}}{\partial L}$, and let $\tilde{W}^D = W^D + (L - \rho)$ and $\tilde{W} = W - \rho$. Next, we demonstrate that $\dot{\tilde{v}} > 0$. From (20),

$$\begin{aligned} \frac{\partial \tilde{v}^3}{\partial L} &= \frac{\partial}{\partial L} \frac{1}{(2K(\sqrt{\tilde{W}} - \sqrt{\tilde{W}^D}))^2} \\ 3\tilde{v}^2 \dot{\tilde{v}} &= \frac{-2}{(2K(\sqrt{\tilde{W}} - \sqrt{\tilde{W}^D}))^3} \left(\frac{1}{2\sqrt{\tilde{W}}} \frac{\partial \tilde{W}}{\partial L} - \frac{1}{2\sqrt{\tilde{W}^D}} \frac{\partial \tilde{W}^D}{\partial L} \right) \\ &= \frac{-2}{(2K(\sqrt{\tilde{W}} - \sqrt{\tilde{W}^D}))^3} \left(\frac{(-\tilde{v}^2 - 2\tilde{v}\dot{\tilde{v}}L)}{2\sqrt{\tilde{W}}} - \frac{(1 - \tilde{v}^2 - 2\tilde{v}\dot{\tilde{v}}L)}{2\sqrt{\tilde{W}^D}} \right) \\ &= \frac{1}{(2K(\sqrt{\tilde{W}} - \sqrt{\tilde{W}^D}))^3} \left(\frac{(\tilde{v}^2 + 2\tilde{v}\dot{\tilde{v}}L)}{\sqrt{\tilde{W}}} + \frac{(1 - \tilde{v}^2 - 2\tilde{v}\dot{\tilde{v}}L)}{\sqrt{\tilde{W}^D}} \right) \\ \therefore \dot{\tilde{v}} &\left(3\tilde{v}^2 + \frac{2\tilde{v}L}{(2K(\sqrt{\tilde{W}} - \sqrt{\tilde{W}^D}))^3} \left[\frac{1}{\sqrt{\tilde{W}^D}} - \frac{1}{\sqrt{\tilde{W}}} \right] \right) \\ &= \frac{1}{(2K(\sqrt{\tilde{W}} - \sqrt{\tilde{W}^D}))^3} \left(\frac{\tilde{v}^2}{\sqrt{\tilde{W}}} + \frac{(1 - \tilde{v}^2)}{\sqrt{\tilde{W}^D}} \right), \end{aligned}$$

where the last step is obtained by moving all the terms involving $\dot{\tilde{v}}$ to the LHS. The RHS is obviously positive while the coefficient of $\dot{\tilde{v}}$ on the LHS is also positive (since $\tilde{W} > \tilde{W}^D$) and $\dot{\tilde{v}} > 0$ is proven.

Next, we differentiate the utility w.r.t. L ,

$$\begin{aligned}
\frac{\partial U}{\partial L} &= \frac{K}{2\sqrt{W - \tilde{v}^2 L}} (-\tilde{v}^2 - 2\tilde{v}\dot{\tilde{v}}L) + \frac{\frac{-1}{3}}{(16K)^{1/3}(\sqrt{W - \tilde{v}^2 L} - \sqrt{W - D + L - \tilde{v}^2 L})^{4/3}} \times \dots \\
&\dots \left(\frac{(-\tilde{v}^2 - 2\tilde{v}\dot{\tilde{v}}L)}{2\sqrt{W - \tilde{v}^2 L}} - \frac{((1 - \tilde{v}^2) - 2\tilde{v}\dot{\tilde{v}}L)}{2\sqrt{W - D + L - \tilde{v}^2 L}} \right) \\
&= \frac{K(-\tilde{v}^2 - 2\tilde{v}\dot{\tilde{v}}L)}{2\sqrt{W - \tilde{v}^2 L}} - \frac{K\tilde{v}^2}{3} \left(\frac{(-\tilde{v}^2 - 2\tilde{v}\dot{\tilde{v}}L)}{2\sqrt{W - \tilde{v}^2 L}} - \frac{((1 - \tilde{v}^2) - 2\tilde{v}\dot{\tilde{v}}L)}{2\sqrt{W - D + L - \tilde{v}^2 L}} \right)
\end{aligned}$$

Collecting the terms and simplifying we obtain:

$$\begin{aligned}
\frac{2}{K} \frac{\partial U}{\partial L} &= \frac{-\tilde{v}^2}{\sqrt{W}} - \frac{2\tilde{v}\dot{\tilde{v}}L}{\sqrt{W}} + \frac{\tilde{v}^2}{3\sqrt{W^D}} - \frac{\tilde{v}^2}{3} \left(\frac{(-\tilde{v}^2 - 2\tilde{v}\dot{\tilde{v}}L)}{\sqrt{W}} - \frac{(-\tilde{v}^2 - 2\tilde{v}\dot{\tilde{v}}L)}{\sqrt{W^D}} \right) \\
&= -\tilde{v}^2 \left(\frac{1}{\sqrt{W}} - \frac{1}{3\sqrt{W^D}} \right) - \frac{2\tilde{v}\dot{\tilde{v}}L}{\sqrt{W}} + \frac{\tilde{v}^2(\tilde{v}^2 + 2\tilde{v}\dot{\tilde{v}}L)}{3} \left(\frac{1}{\sqrt{W}} - \frac{1}{\sqrt{W^D}} \right) \\
&= -\tilde{v}^2 \left(\frac{3\sqrt{W^D} - \sqrt{W}}{3\sqrt{W}\sqrt{W^D}} \right) - \frac{2\tilde{v}\dot{\tilde{v}}L}{\sqrt{W}} + \frac{\tilde{v}^2(\tilde{v}^2 + 2\tilde{v}\dot{\tilde{v}}L)}{3} \left(\frac{\sqrt{W^D} - \sqrt{W}}{\sqrt{W}\sqrt{W^D}} \right) \quad (26)
\end{aligned}$$

Since $2\tilde{v}\dot{\tilde{v}}L > 0$ and $\sqrt{W^D} < \sqrt{W}$, the last two terms of (26) are strictly negative for any $L \geq 0$.

Let $D < \frac{8}{9}W$. Then, $W < 9(W - D)$, and taking the square root we obtain:

$$3\sqrt{W^D} - \sqrt{W} > 0, \quad (27)$$

and since $\tilde{W}^D = W^D + (L^\ddagger - \rho^\ddagger) > W^D$ and $\tilde{W} = W - \rho < W$ from (27) we have:

$$3\sqrt{\tilde{W}^D} - \sqrt{\tilde{W}} > 3\sqrt{W^D} - \sqrt{W} > 0.$$

Hence, we have proven that if $D < \frac{8}{9}W$, $3\sqrt{\tilde{W}^D} - \sqrt{\tilde{W}} > 0$. In this case, the first term of (26) is negative as well, which leads to:

$$\frac{2}{K} \frac{\partial U}{\partial L} < 0.$$

Thus, we have proven that if $D < \frac{8}{9}W$, utility is maximized at $L = 0$. Thus, the only equilibrium insurance contract is $(0, 0)$.

If $D > \frac{8}{9}W$, there could exist an insurance contract, which improves user utility relative to U^* . See Fig. 2(a) for an example which shows how $U(\rho, L)$ is maximized at $L > 0$, and users may reach a higher utility with insurance.

Proof of Proposition 3

First, we notice that in any equilibrium, $L^\dagger = D$ and insurer profit is zero due to competition, as in Proposition 2. Hence, we restrict our analysis to full coverage only.

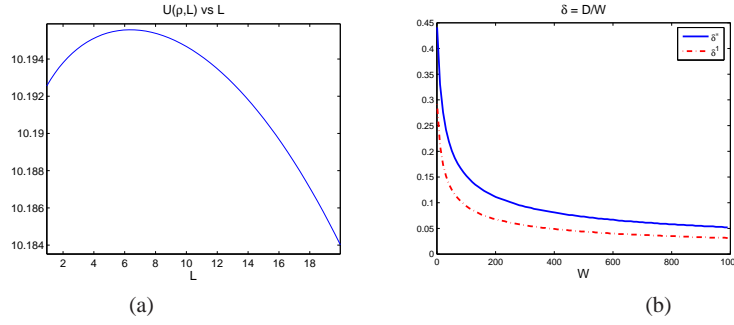


Fig. 2 (a) Unobservable case: U vs L ($L \in [0, 20]$, $K = 1$, $W = 100$, $D = 99$) and (b) Observable case: δ^\dagger and δ^1 vs W .

Second, in any equilibrium, user utility from deviation to no-insurance gives user a strictly lower utility. Indeed, assume the reverse. Suppose a user can deviate to v_i with no insurance and his utility without insurance is equal to his utility with insurance, i.e., $U(v_i, v_i^\dagger, 0, 0) \geq U(v_i^\dagger, v_i^\dagger, v_i^{\dagger 2}D, D)$. Consider an entrant insurer who offers him a contract $(v_i, v_i v_i^\dagger D, D)$ that offers non-zero coverage at actuarially fair price. By adopting this contract, the user improves his utility, which conflicts our assumption about the equilibrium. Therefore, the utility from deviation must be strictly lower and all users strictly prefer to buy insurance.

Lastly, we prove that in any equilibrium, all user contracts are identical. Assume the reverse, and let $(v_1, v_1 \bar{v}D, D)$ and $(v_2, v_2 \bar{v}D, D)$ be two contracts in equilibrium, with non-zero fraction of users buying each contract. Without loss of generality, we let $v_1 < v_2$, and thus $v_1 < \bar{v} < v_2$. From Section 3.2.2, we assume that insurers take \bar{v} as given. Consider the contract $(\tilde{v}, \tilde{v} \bar{v}D, D)$ offered by an entrant insurer. Suppose this contract maximizes $U(\tilde{v}, \tilde{v} \bar{v}D, D)$:

$$\frac{\partial}{\partial \tilde{v}} (\sqrt{\tilde{v}} + K\sqrt{W - \tilde{v}\bar{v}D}) = 0.$$

$$\begin{aligned} \frac{\partial}{\partial \tilde{v}} (\sqrt{\tilde{v}} + K\sqrt{W - \tilde{v}\bar{v}D}) &= 0 \\ \frac{1}{2\sqrt{\tilde{v}}} - \frac{K\bar{v}D}{2\sqrt{W - \tilde{v}\bar{v}D}} &= 0 \\ \frac{\sqrt{W - \tilde{v}\bar{v}D}}{\sqrt{\tilde{v}}} &= K\bar{v}D \end{aligned} \quad (28)$$

From (28), there is a unique solution for \tilde{v} since the LHS is monotone decreasing. Hence, $\tilde{v} \neq v_1$ and $\tilde{v} \neq v_2$ since if either were true, then $U(v_1, v_1 \bar{v}D, D) \neq U(v_2, v_2 \bar{v}D, D)$, which is a contradiction. Thus, $U(\tilde{v}, \tilde{v} \bar{v}D, D) > U(v_1, v_1 \bar{v}D, D) = U(v_2, v_2 \bar{v}D, D)$ and insured users will be willing to deviate to this new contract.

Thus, we have shown that two different contracts cannot be present in equilibrium, and we have proven that in any equilibrium, all users buy an identical contract.

Next, we prove that the equilibrium is unique. From (28), in any equilibrium, $\bar{v} = \bar{v} = v^\dagger$, and we have

$$\begin{aligned}\frac{\sqrt{W - v^{\dagger 2}D}}{\sqrt{v^\dagger}} &= K v^\dagger D \\ \sqrt{W - v^{\dagger 2}D} &= K v^\dagger \sqrt{v^\dagger} D \\ \frac{v^{\dagger 3}}{W - v^{\dagger 2}D} &= \frac{1}{(KD)^2}.\end{aligned}\tag{29}$$

From (29), there is a unique solution for the equilibrium v^\dagger , since the LHS is monotone decreasing. Thus, the equilibrium is unique.

Next, we determine how this unique v^\dagger compares to v^* . When both v^\dagger and $v^* < 1$, we can equate v^3 from (9) and (29) to get

$$\begin{aligned}\frac{1}{[2K(\sqrt{W} - \sqrt{W-D})]^2} &= \frac{W - v^2D}{(KD)^2} \\ \frac{D^2}{[2(\sqrt{W} - \sqrt{W-D})]^2} &= W - v^2D \\ \frac{W}{D} - \frac{D}{[2(\sqrt{W} - \sqrt{W-D})]^2} &= v^2\end{aligned}$$

Using (9) for $v^* < 1$ and denoting $\frac{D}{W}$ by δ , we have

$$\begin{aligned}\frac{W}{D} - \frac{D}{[2(\sqrt{W} - \sqrt{W-D})]^2} &= \frac{1}{[2K(\sqrt{W} - \sqrt{W-D})]^{4/3}} \\ \frac{1}{\frac{D}{W}} - \frac{\frac{D}{W}}{[2(1 - \sqrt{1 - \frac{D}{W}})]^2} &= \frac{1}{[2K\sqrt{W}(1 - \sqrt{1 - \frac{D}{W}})]^{4/3}} \\ \frac{1}{\delta} - \frac{\delta}{[2(1 - \sqrt{1 - \delta})]^2} &= \frac{1}{[2K\sqrt{W}(1 - \sqrt{1 - \delta})]^{4/3}}.\end{aligned}$$

Thus, we obtain an equation for δ :

$$\begin{aligned}(1 - \sqrt{1 - \delta})^{1/3} \left(\frac{(1 - \sqrt{1 - \delta})}{\delta} - \frac{\delta}{4(1 - \sqrt{1 - \delta})} \right) &= \frac{1}{[2K\sqrt{W}]^{4/3}} \\ (1 - \sqrt{1 - \delta})^{1/3} \left(\frac{1}{(1 + \sqrt{1 - \delta})} - \frac{(1 + \sqrt{1 - \delta})}{4} \right) &= \frac{1}{[2K\sqrt{W}]^{4/3}}\end{aligned}\tag{30}$$

We observe that the LHS is an increasing function of δ , which gives us a unique solution δ^* of (30). For $\delta \leq \delta^*$, we have $v^\dagger \leq v^*$, i.e., insurance improves the security level in the no-insurance Nash equilibrium. From (9), we know that when δ is

low, v^* is high. This implies that insurance improves upon the no-insurance security level only when v^* is high. Let δ^1 denote the δ at which $v^* = 1$. Fig. 2 (b) depicts δ^1 and δ^* as a function of the wealth W ($K = 1$).

Social Planner

The contract offered by a social planner must be a solution to the following optimization problem:

$$\begin{aligned} \max_{v, \rho, L} \quad & U(v, v, \rho, L) \\ \text{s.t.} \quad & v^2 L \leq \rho \text{ and } v \leq 1. \end{aligned}$$

Next, we write the Lagrangian:

$$LAN = U(v, v, \rho, L) - \lambda_1(v^2 L - \rho) - \lambda_2(v - 1)$$

Taking the derivatives of LAN w.r.t. v , L and ρ and equating to 0 gives us the following equations.

$$\begin{aligned} \frac{\partial LAN}{\partial v} &= \frac{\partial U(v, v, \rho, L)}{\partial v} - 2\lambda_1 v L - \lambda_2 = 0 \\ \left(\frac{1}{2\sqrt{v}} - 2vK(\sqrt{W - \rho} - \sqrt{W - D + L - \rho})\right) - 2\lambda_1 v L - \lambda_2 &= 0 \end{aligned} \quad (31)$$

$$\begin{aligned} \frac{\partial LAN}{\partial L} &= \frac{\partial U(v, v, \rho, L)}{\partial L} - \lambda_1 v^2 = 0 \\ \frac{Kv^2}{2\sqrt{W - D + L - \rho}} - \lambda_1 v^2 &= 0 \end{aligned} \quad (32)$$

$$\begin{aligned} \frac{\partial LAN}{\partial \rho} &= \frac{\partial U(v, v, \rho, L)}{\partial \rho} + \lambda_1 = 0 \\ -\frac{Kv^2}{2\sqrt{W - D + L - \rho}} - \frac{K(1 - v^2)}{2\sqrt{W - \rho}} + \lambda_1 &= 0 \end{aligned} \quad (33)$$

Further, from complementary slackness, we have

$$\lambda_1(v^2 L - \rho) = 0, \quad (34)$$

$$\text{and } \lambda_2(v - 1) = 0 \quad (35)$$

Note that $v \neq 0$, since that would require infinite security costs for the users. From (32), we conclude that $\lambda_1 > 0$ and thus the constraint (34) binds:

$$v^2 L = \rho \quad (36)$$

Equating λ_1 from (32) and (33), we obtain:

$$\frac{K}{2\sqrt{W-D+L-\rho}} = \frac{Kv^2}{2\sqrt{W-D+L-\rho}} + \frac{K(1-v^2)}{2\sqrt{W-\rho}}$$

Canceling out $K/2 > 0$, we obtain:

$$\frac{1}{\sqrt{W-D+L-\rho}} = \frac{v^2}{\sqrt{W-D+L-\rho}} + \frac{(1-v^2)}{\sqrt{W-\rho}},$$

or

$$\frac{(1-v^2)}{\sqrt{W-D+L-\rho}} = \frac{(1-v^2)}{\sqrt{W-\rho}},$$

which leads to:

$$L = D \text{ if } v < 1. \quad (37)$$

Now, if $v < 1$, we can substitute (36) and (37) into (32) to get $\lambda_1 = \frac{K}{2\sqrt{W-v^2D}}$. Substituting this value of λ_1 , $\lambda_2 = 0$ (since $v < 1$) and (37) into (31), we get

$$\begin{aligned} \frac{1}{2\sqrt{v}} &= \frac{K}{\sqrt{W-v^2D}} vD \\ \frac{v^3}{W-v^2D} &= \frac{1}{(2KD)^2} \end{aligned} \quad (38)$$

Thus, if $v < 1$, it is the unique solution to (38) (since the LHS is monotone increasing).

References

1. Akerlof, G.A.: The market for 'lemons': Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics* **84**(3), 488–500 (1970). URL <http://ideas.repec.org/a/tpr/qjecon/v84y1970i3p488-500.html>
2. Anderson, R., Böhme, R., Clayton, R., Moore, T.: Security economics and european policy. In: Proceedings of WEIS'08. Hanover, USA (2008)
3. Baer, W.S., Parkinson, A.: Cyberinsurance in it security management. *IEEE Security and Privacy* **5**(3), 50–56 (2007). DOI <http://dx.doi.org/10.1109/MSP.2007.57>
4. Böhme, R.: Cyber-insurance revisited. In: Proceedings of WEIS'05. Cambridge, USA (2005)
5. Bolot, J., Lelarge, M.: A new perspective on internet security using insurance. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE pp. 1948–1956 (2008). DOI 10.1109/INFOCOM.2008.259
6. Fisk, M.: Causes and remedies for social acceptance of network insecurity. In: Proceedings of WEIS'02. Berkeley, USA (2002)
7. Gordon, L.A., Loeb, M., Sohail, T.: A framework for using insurance for cyber-risk management. *Communications of the ACM* **46**(3), 81–85 (2003)
8. Gordon, L.A., Loeb, M.P.: The economics of information security investment. *ACM Trans. Inf. Syst. Secur.* **5**(4), 438–457 (2002). DOI <http://doi.acm.org/10.1145/581271.581274>
9. Grossklags, J., Christin, N., Chuang, J.: Secure or insure?: a game-theoretic analysis of information security games. In: WWW '08: Proceeding of the 17th international con-

- ference on World Wide Web, pp. 209–218. ACM, New York, NY, USA (2008). DOI <http://doi.acm.org/10.1145/1367497.1367526>
10. H. Ogut, N.M., Raghunathan, S.: Cyber insurance and it security investment: Impact of interdependent risk. In: Proceedings of WEIS'05. Cambridge, USA (2005)
 11. Hausken, K.: Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers* **8**(5), 338–349 (2006). DOI <http://dx.doi.org/10.1007/s10796-006-9011-6>
 12. Hofmann, A.: Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks. *Geneva Risk and Insurance Review* **32**(1), 91–111 (2007)
 13. Honeyman, P., Schwartz, G., Assche, A.V.: Interdependence of reliability and security. In: Proceedings of WEIS'07. Pittsburg, PA (2007)
 14. Kunreuther, H., Heal, G.: Interdependent security. *Journal of Risk and Uncertainty* **26**(2-3), 231–49 (2003). URL <http://ideas.repec.org/a/kap/jrisku/v26y2003i2-3p231-49.html>
 15. Kunreuther, H.C., Michel-Kerjan, E.O.: Evaluating the effectiveness of terrorism risk financing solutions. NBER Working Papers 13359, National Bureau of Economic Research, Inc (2007). URL <http://ideas.repec.org/p/nbr/nberwo/13359.html>
 16. Majuca, R.P., Yurcik, W., Kesan, J.P.: The evolution of cyberinsurance. Tech. Rep. CR/0601020, ACM Computing Research Repository (2006)
 17. Rothschild, M., Stiglitz, J.E.: Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. *The Quarterly Journal of Economics* **90**(4), 630–49 (1976). URL <http://ideas.repec.org/a/tpr/qjecon/v90y1976i4p630-49.html>
 18. Schechter, S.E.: Computer security strength and risk: a quantitative approach. Ph.D. thesis, Cambridge, MA, USA (2004). Adviser-Smith, Michael D.
 19. Soohoo, K.: How much is enough? a risk-management approach to computer security. Ph.D. thesis, Stanford University
 20. Stiglitz, J.E.: Information and the change in the paradigm in economics. *American Economic Review* **92**(3), 460–501 (2002). URL <http://ideas.repec.org/a/aea/aecrev/v92y2002i3p460-501.html>
 21. Varian, H.: System reliability and free riding. In: Workshop on the Economics of Information Security, WEIS 2002. Cambridge, USA (2002)