高技术通讯 2016 年 第26卷 第8－9期:732～738

doi:10.3772/j.issn.1002-0470.2016.08－09.004

道德风险条件下的最优网络安全保险契约模型研究①

杨云雪②*** 王燕霞***

(*中国科学院网络数据科学与技术重点实验室,中国科学院计算技术研究所 北京 100190)

(**中国科学院大学 北京 100049)

摘 要 针对信息非对称性导致网络安全保险市场运行效率下降问题,进行了网络用户道德风险条件下的最优网络安全保险契约模型研究,使用委托代理理论建立了此类网络安全保险契约分析模型并对其性质进行了讨论。证明了不存在网络用户道德风险时,最优网络安全保险契约可以实现风险分担的帕累托最优并要求完全保险,此时最优网络安全保险费等于网络安全事件造成损失的期望值;存在网络用户道德风险时,最优网络安全保险契约不能达到风险分担的帕累托最优并要求部分保险,此时最优网络安全保险费小于网络安全事件造成损失的期望值。

关键词 网络安全保险,道德风险,保险契约,信息非对称性,帕累托最优

0 引 言

长期以来,尽管工业界和学术界都研究并开发了许多先进的网络安全防护工具,但是实现理想的网络安全保护仍非常困难[1]。针对该问题,研究人员提出一种新形式的网络安全风险管理方式——网络安全保险。网络用户购买网络安全保险就是把自身风险转移给网络安全保险公司,被攻击后造成的损失由网络安全保险公司赔偿,而网络安全保险公司则向网络用户收取保险费。由于通常的自我安全防御技术不能完全消除风险,因此网络安全保险是一种转移网络用户安全剩余风险的有效工具。

理想的网络安全保险契约保证网络安全保险公司的利润,是网络安全保险市场持续发展下去的关键[2]。然而,信息非对称性作为保险机制的固有特征很容易导致保险市场运行的低效率,最终导致保险市场失灵的局面。在网络安全保险中,发生在网络用户投保之前的信息非对称导致网络用户逆向选择问题;发生在网络用户投保之后的信息非对称导致网络用户道德风险问题。为了改善信息非对称性对网络安全保险市场交易效率的影响,本进行了网络用户道德风险条件下的最优网络安全保险契约模型研究,使用委托代理理论建立了此类最优保险契约分析模型。另外,由于委托代理理论的中心问题是"保险"和"激励"的交替问题[3,4],因此作为分析的第一步,我们首先讨论了不存在网络用户道德风险情况下的最优网络安全保险契约模型,然后再引入非对称信息说明存在激励问题时,如何建立道德风险条件下的最优网络安全保险契约模型。本文的主要贡献在于:(1)使用委托代理理论建立最优网络安全保险契约模型,把网络用户的自我安全防御努力水平设计为一维连续变量,从而克服了已有模型中网络用户只有两种自我安全防御行动选择的局限性。(2)提出了不存在网络用户道德风险情况下的最优网络安全保险契约模型,证明了不存在道德风险时,最优网络安全保险契约可以实现风险分担的帕累托最优并要求完全保险。(3)提出了存在网

① 国家自然科学基金(61402437)和863计划(2015AA016005)资助项目。

② 女,1986年生,博士生;研究方向:网络安全保险,安全风险评估,安全态势感知;联系人,E-mail: yangyunxue@software.ict.ac.cn

(收稿日期:2016-07-04)

络用户道德风险情况下的最优网络安全保险契约模型,证明存在道德风险时,最优网络安全保险契约不能达到风险分担的帕累托最优和要求部分保险。

1 相关工作

在信息非对称性对网络安全保险市场造成的影响研究方面,Lelarge 等人[5,6]的研究结果表明,信息非对称性存在的情况下,网络安全保险无法激励实体的自我安全防御投资以及信息非对称性不存在的情况下,网络安全保险能够激励实体的自我安全防御投资,从而引起级联效应,使得其他实体进行自我安全防御投资。他们认为网络安全保险提高了自我安全防御水平,进一步提高了网络安全性水平;网络安全保险应该成为互联网风险管理的重要组成部分[7-9]。Schwartz 等人[10]研究了竞争性的网络安全保险市场对网络安全性和网络社会福利的影响,说明了信息不对称性会导致网络安全保险市场失灵以及信息不对称性不存在时,网络安全保险能够提高用户的福利但无法提高网络安全性。Schwartz 等人在另一项研究工作中[11]研究了逆向选择问题对网络安全保险市场的影响,把风险厌恶的网络用户分为正常用户和恶意用户,说明了逆向选择问题会导致网络安全保险契约不能反映出投保人的真实安全性,证明了逆向选择问题会降低网络安全保险市场的交易效率,最终导致网络安全保险市场消失。Pal 等人[12]针对逆向选择对网络安全保险市场造成负面影响问题,提出了一种分离式网络安全保险契约设计方法。该方法的提出基于用户最优安全防御投资与网络外部性成比例的研究结果,鼓励风险类型不同的网络用户选择适合自己风险类型的保险契约,进而缓解了逆向选择问题对网络安全保险市场造成的负面影响。Yang 等人[13]研究了道德风险问题对网络安全保险市场的影响,说明道德风险问题不存在时,网络安全保险能够激励自我安全防御技术的采用以及道德风险问题存在时,网络安全保险无法激励自我安全防御技术的采用但能够提高网络用户的效用。

在网络安全保险契约研究方面,Pal 等人[14]提出了一个网络安全保险市场供需模型,说明了混合合同无法提高用户安全性,分离合同能够提高用户安全性,但是网络安全保险公司的期望利润为零。针对如何提高网络安全保险公司利润问题,Pal 等人[15]在另外一项研究工作中把风险规避的安全产品供应商建模成网络安全保险公司并基于用户逻辑网络和用户安全投资额提出一个单期静态定价策略和一个离散事件连续的动态定价策略。Herath 等人[16]提出了一种基于连接函数的网络安全保险费计算方法。在计算网络安全保险费时该方法涵盖了保险合同的三个基本要素——保险赔偿金、保险费和保险责任开始的时间并抓住了输入变量之间的非线性依赖关系。Mukhopadhyay 等人[17]提出了一个基于效用的优惠定价模型,该模型使用集体风险模型并基于企业的期望损失、风险态度和财务状况计算网络安全保险费。

综上所述,理想的网络安全保险契约是提高网络安全保险市场运行效率、保证网络安全保险公司利润、进一步保证网络安全保险业务快速增长的关键。网络安全保险契约中既存在激励问题,又存在信息非对称性问题,但是已有的网络安全保险契约设计研究都没有同时考虑这两个问题,因此没有设计出信息非对称性存在情况下的最优网络安全保险契约。

2 网络安全保险基础

本节介绍与网络安全保险有关的基本经济学概念。

(1) 网络安全保险:是一种新形式的网络安全风险管理方式,把网络用户的风险转移给网络安全保险公司。网络用户被攻击后造成的损失由网络安全保险公司赔偿,而网络安全保险公司则向网络用户收取保险费。

(2) 自我安全防御:是指用户为了提高网络安全性,购买和使用网络安全技术,如入侵检测系统、防火墙、杀毒软件、反垃圾邮件技术等。

(3) 网络安全保险契约:也称为网络安全保险合同,是网络用户(投保人)与网络安全保险公司

(保险人)之间设立、变更、终止保险法律关系的协议。

(4) 网络安全保险费:是指网络用户(投保人)购买网络安全保险时,根据保险契约所订的保险费率,向网络安全保险公司(保险人)交付的费用。

(5) 网络安全保险费率:是网络安全保险费与网络安全保险金额的比例。

(6) 网络安全保险金额:是指一个网络安全保险合同项下,网络安全保险公司承担赔偿或给付保险金责任的最高限额,即网络用户(投保人)对保险对象的实际投保金额。

(7) 网络用户安全风险倾向:也称为网络用户安全风险态度,分为三种类型——安全风险爱好、安全风险厌恶和安全风险中性。安全风险爱好是指网络用户在进行投资时对具有同一期望报酬的投资宁愿选择安全风险程度更大的投资;安全风险厌恶是指网络用户在进行投资时偏好安全性而对安全风险持不喜欢态度;安全风险中性是指网络用户在进行投资时并不介意投资是否具有比较确定或者不那么确定的结果,只要期望效用最大化即可。

(8) 信息不对称性:是指购买网络安全保险的网络用户与网络安全保险公司对网络安全风险信息的了解具有差异性。

(9) 道德风险:是指网络安全保险公司由于不能观察到网络用户购买网络安全保险后的自我安全防御措施,从而网络用户的自我安全防御行为可能损害到网络安全保险公司利益的风险。

(10) 逆向选择:是指网络安全保险公司在签约前不了解网络用户的安全风险水平,从而导致网络安全保险不能达到对称信息时的最优程度的现象。

3 最优网络安全保险契约模型

本节主要研究网络用户道德风险情况下的最优网络安全保险契约模型。作为分析的第一步,首先讨论不存在网络用户道德风险情况下的最优网络安全保险契约模型。这是因为"保险"和"激励"的交替问题是委托代理关系的中心问题,不存在道德风险时,本文可以孤立地考虑最优的风险分担问题;在完成这一步后再引入道德风险是为了便于说明存在激励问题时,帕累托最优的风险分担不能达到[3,4]。

3.1 基本模型和假设

考虑一个网络群体有 N 个同样的网络用户[1,10],假设每个网络用户的初始财富为 w_0;网络安全事件给每个网络用户造成的经济损失为 $l \geqslant 0$,且 l 为一个随机变量,其分布函数为 $P(l)$,分布密度为 $p(l)$,那么 $l = 0$,即网络用户不发生网络安全事件的概率为 $p(0)$,而且 $l > 0$ 时,$p(l)$ 是连续的,又有 $P(0) > 0$;网络安全保险费率为 δ,投保金额为 π,那么 $\delta\pi$ 即为网络安全保险公司向网络用户应收的网络安全保险费;当网络安全事件发生时,网络用户从网络安全保险公司获得的赔偿费为 $g(l) \geqslant 0$ 且 $g(l) \leqslant l$(如果 $g(l) = l$ 则称为足额网络安全保险;$g(l) < l$ 则称为不足额网络安全保险;$g(l) > l$ 则称为超额网络安全保险),即不存在超额网络安全保险的情况;如果发生了损失,即 $l > 0$ 时 $g(l) > 0$;网络用户的效用函数为 $u(x)$,不妨设 $u(0) = 0$,并且网络用户为安全风险厌恶型的,即 $u' > 0, u'' < 0$。有了上面的假设,网络用户的期望效用函数可以表示如下:

$$p(0)u(w_0 - \delta\pi) + \int_{l>0} u(w_0 + g(l) - l - \delta\pi)p(l)dl \tag{1}$$

如何选择 $g(l)$ 和 δ 使得上述期望效用函数最大化是网络用户面临的问题。下面,本研究首先基于委托代理理论建立信息对称情况下,不存在网络用户道德风险时的最优网络安全保险契约模型,然后再建立信息非对称情况下,网络用户道德风险存在时的最优网络安全保险契约模型。

3.2 不存在网络用户道德风险时的最优网络安全保险契约模型

我们先来考虑一种理想情况,即网络用户的行为不会影响网络安全事件的发生和遭受经济损失的大小,下面用委托代理理论来分析这种情况下的最优网络安全保险契约。

当网络用户选择 $g(l)$ 和 δ 最大化式(1)期望效用函数时,面临着网络安全保险公司赢利的约束。因此,我们建立如下的基于委托代理理论的最优网络安全保险契约模型:

$$\max_{g(l),\delta} p(0)u(w_0-\delta\pi)+\int_{l>0}u(w_0+g(l)-l-\delta\pi)p(l)dl \quad s.t.\ \delta\pi-\int_{l>0}g(l)p(l)dl\geqslant 0 \quad (2)$$

模型中的约束条件是网络安全保险公司的赢利约束,即参与约束。进一步,我们假设网络安全保险市场是完全竞争的,即竞争使得网络安全保险活动无法给网络安全保险公司提供超额利润,如果存在交易的剩余,则完全被网络用户占有。则上述最优化问题中约束条件中的等号成立。

显然,我们建立的模型没有考虑委托代理模型中的代理人参与约束,即网络用户购买网络安全保险后的期望效用水平比没有购买网络安全保险时的期望效用水平高,这是因为我们建立的模型中已经确保在满足委托人,即网络安全保险公司的参与约束的条件下,最大化网络用户购买网络安全保险后的期望效用。因此,我们建立的以上模型实际上已经在可保网络安全风险的范围内包含了代理人,即网络用户的参与约束。

定理 1 当网络用户道德风险不存在,即网络用户与网络安全保险公司信息对称时,最优网络安全保险契约可以实现风险分担的帕累托最优。

证明:针对以上的最优化问题,构造拉格朗日函数如下:

$$L(g(l),\delta)=p(0)u(w_0-\delta\pi)+\int_{l>0}u(w_0+g(l)-l-\delta\pi)p(l)dl+\lambda(\delta\pi-\int_{l>0}g(l)p(l)dl) \quad (3)$$

令 $w_n=w_0-\delta\pi$, $w_m=w_0+g(l)-l-\delta\pi$, 则

$$L(g(l),\delta)=p(0)u(w_n)+\int_{l>0}u(w_m)p(l)dl+\lambda(\delta\pi-\int_{l>0}g(l)p(l)dl) \quad (4)$$

对于网络安全赔偿方案 $g(l)$ 和网络安全保险费率 δ 的一阶条件分别为

$$u'(w_m)-\lambda=0 \quad (5)$$

$$p(0)u'(w_n)+\int_{l>0}u'(w_m)p(l)dl=\lambda \quad (6)$$

由于约束条件的等号成立,根据库恩-塔克条件可知 λ 为一个正的常数,因此式(6)正是帕累托最优。故最优网络安全保险契约一定实现帕累托最优的风险分担。

定理 2 在没有网络用户道德风险的情况下,网络用户投保后如果网络安全事件发生,则遭受的实际损失 $g(l)-l$ 与 l 无关,而且最优网络安全保险契约要求完全保险;最优网络安全保险费 $\delta\pi$ 等于所受损失的期望值 $E(l)$。

证明:由于 $\int_{l>0}\lambda p(l)dl=\lambda(1-p(0))$, 其中 $p(0)$ 为不发生网络安全事件的概率,再将式(5)带入式(6)可得: $u'(w_n)-\lambda=0$。因为 λ 是一个正的常数,显然有 $w_m=w_n$, 且 $w_m=w_n$ 为一常数,即可得

$$g(l)-l=0 \quad (7)$$

又有 $\int_{l>0}lp(l)dl=E(l)$, 再将式(7)带入约束条件就有 $\delta\pi=E(l)$, 即 $\delta=\frac{E(l)}{\pi}$。

证毕

从上面的分析可见,在网络用户的行为不会影响网络安全事件的发生和遭受经济损失的大小的情况下,最优网络安全保险契约要求完全保险,即在网络安全事件发生后,网络用户将获得全部赔偿。另外,网络安全保险公司的风险态度为中性导致其向网络用户收取的保险费恰好等于损失变量的期望值。因此,不存在网络用户道德风险的情况下,最优网络安全保险契约实现了帕累托最优的风险分担。

3.3 存在网络用户道德风险时的最优网络安全保险契约模型

当网络安全保险市场中存在道德风险问题时,网络安全保险公司无法观测到网络用户在投保后是否采取了自我安全防御措施(如防火墙、入侵检测系统、防病毒软件等),从而网络用户的自我安全防御措施偏离没有网络安全保险时的情况,即网络用户的行为会影响网络安全事件的发生。此时,激励网络用户采取自我安全防御措施是设计此类网络安全保险契约时需要考虑的问题。下面进行具体分析。

已有模型中,网络用户只有两种自我安全防御行动选择[13]。从经济学的角度讲,尽管只有两种自我安全防御行动选择的简单模型已经包含了委托-

代理理论的基本结论,但是考虑连续变量的一般模型具有更重要的方法论意义[3]。

本文用 a 表示网络用户在自我安全防御措施方面付出的努力水平,并且假设 a 是一维连续变量。$c(a)$ 为网络用户的努力负效用,且有 $c'>0, c''>0$。由于考虑到网络用户的行动会影响网络安全事件所引起的损失的大小,因此我们假设网络安全事件所造成的损失 l 的分布函数为 $P(l,a)$,分布密度为 $p(l,a)(l\geqslant 0)$。网络用户付出的努力越多意味着网络安全事件造成的损失就可能越小。针对这一点,我们用一阶随机占优条件 $P_a(l,a)>0$ 表示,即 a 越大,某一损失水平 l 发生的概率就越小。再假设 $l=0$ 即不发生损失时,$P(0,a)>0$ 且 $P_a(0,a)>0$,意味着网络用户在自我安全防御措施方面付出的努力水平越高,网络安全风险损失发生的概率就越小,但网络安全风险损失发生的边际概率递增;$l>0$ 时,$p(l,a)$ 对 l 连续、对 a 可导且 $p_a(l,a\mid l>0)<0$,即网络用户的努力水平越高,发生风险损失 l 的概率越小。

当道德风险问题存在时,使用委托代理模型建立保险契约时就要考虑激励相容约束。于是可以建立如下的最优网络安全保险契约模型:

$$\max_{\delta,g(l),a} p(0,a)u(w_0-\delta\pi)+\int_{l>0}u(w_0+g(l)-l-\delta\pi)p(l,a)dl-c(a) \tag{8}$$

s. t.

$$\delta\pi-\int_{l>0}g(l)p(l,a)dl=0 \tag{9}$$

$$a=\arg\max_a\left[p(0,a)u(w_0-\delta\pi)+\int_{l>0}u(w_0+g(l)-l-\delta\pi)p(l,a)dl-c(a)\right] \tag{10}$$

如文献[3]中所述,本文可以用一阶条件来替换上述模型中的第二个约束条件,即

$$p_a(0,a)u(w_0-\delta\pi)+\int_{l>0}u(w_0+g(l)-l-\delta\pi)p_a(l,a)dl=c'(a) \tag{11}$$

于是,原模型可写为

$$\max_{\delta,g(l),a} p(0,a)u(w_0-\delta\pi)+\int_{l>0}u(w_0+g(l)-l-\delta\pi)p(l,a)dl-c(a) \tag{12}$$

s. t.

$$\delta\pi-\int_{l>0}g(l)p(l,a)dl=0 \tag{13}$$

$$p_a(0,a)u(w_0-\delta\pi)+\int_{l>0}u(w_0+g(l)-l-\delta\pi)p_a(l,a)dl=c'(a) \tag{14}$$

因此,网络用户道德风险存在时的最优网络安全保险契约模型可以表示为由式(12)、(13)和(14)组成的最优化问题,式(12)为目标函数,式(13)和式(14)为约束条件。针对上述问题构造拉格朗日函数,同时令 $w_n=w_0-\delta\pi, w_m=w_0+g(l)-l-\delta\pi$,有

$$\begin{aligned}L(g(l),\delta)=&\,p(0,a)u(w_n)+\int_{l>0}u(w_m)p(l,a)dl-c(a)+\lambda\left(\delta\pi-\int_{l>0}g(l)p(l,a)dl\right)\\&+\mu\left(p_a(0,a)u(w_n)+\int_{l>0}u(w_m)p_a(l,a)dl-c'(a)\right)\end{aligned} \tag{15}$$

对于赔偿方案 $g(l)$ 的一阶条件为

$$u'(w_m)-\lambda+\mu u'(w_m)\frac{p_a(l,a)}{p(l,a)}=0 \tag{16}$$

其中 λ 为正常数,并且由于激励相容约束作用,μ 不能为 0。显然有

$$u'(w_m)=\frac{\lambda}{1+\mu\dfrac{p_a(l,a)}{p(l,a)}} \tag{17}$$

其中 $\dfrac{p_a(l,a)}{p(l,a)}$ 为概率密度函数 $p(l)$ 的似然函数,由于拉格朗日乘子 λ 为正常数,而且 $\mu\neq 0$,因此当似然函数不是一个常数函数时,式(17)右端必不是一个常数。

通过以上分析,我们可以得到如下定理。

定理 3 当网络用户道德风险存在时,最优网络安全保险契约不能实现帕累托最优的风险分担,即此时的最优网络安全保险契约不是帕累托最优保险契约。

由定理 3 可知,网络用户道德风险问题造成此时最优网络安全保险契约不能使网络用户与网络安全保险公司之间实现帕累托最优风险分担。因此此时的最优网络安全保险契约要求网络用户为自己的网络安全状况承担风险。

定理 4 在网络安全保险公司为风险中性,网络用户为风险厌恶型的条件下,如果网络安全事件所造成损失的分布密度函数满足单调似然率特征:$\frac{p_a}{p}$ 是损失 l 的递减函数,即较小的 l 意味着网络用户在自我安全防御措施方面付出较大的努力水平。那么网络安全事件发生后,网络用户遭受的实际损失 $l-g(l)$ 是网络安全事件造成损失的递增函数,此时的最优网络安全保险费 $\delta\pi$ 小于损失的期望值 $E(l)$。

证明:保险费率 δ 的一阶条件为

$$p(0,a)u'(w_n)+\int_{l>0}u'(w_m)p(l,a)dl+\mu(p_a(0,a)u'(w_n)+\int_{l>0}u'(w_m)p_a(l,a)dl)=\lambda$$

由于 $\int_{l>0}p(l,a)dl=1-p(0,a)$,再将式(17)带入上式,可得

$$u'(w_n)=\frac{\lambda p(0,a)}{p(0,a)+\mu p_a(0,a)} \tag{18}$$

由于(18)式右边是一个与 l 无关的常数,因此网络安全保险费 $\delta\pi$ 也是与 l 无关的常数,可以写作 $\delta\pi=k$,即网络安全保险费率与投保金额成反比。

当网络安全事件造成的损失增大时,根据单调似然率特征,得到 $\frac{p_a}{p}$ 变小,由式(17)可得 $u'(w_m)$ 变大,因为 $u'(w_m)$ 是网络用户所受实际损失 $l-g(l)+\delta\pi$ 的递增函数,由上面的证明可知 $\delta\pi$ 是与 l 无关的常数,所以有 $l-g(l)$ 变大。再由第一个约束条件 $\delta\pi-\int_{l>0}g(l)p(l,a)dl=0$,以及 $g(l)<l$ 和如下关系:$E(l)=\int_{l>0}lf(l,a)dl$,可得 $\delta\pi<E(l)$。可见,存在道德风险时,网络用户购买网络安全保险时所应缴纳的保险费率也变小。

证毕

根据定理 4 可知,网络安全事件发生时,即 $l>0$ 时,必然有 $g(l)<l$,即最优网络安全保险契约要求部分保险。$g(l)$ 与 l 之间的差距随着网络安全事件造成的损失 l 的增大而增大。从现实意义上讲,定理 4 的结论为激励网络用户采取自我安全防御措施提供了重要依据,从而有效地制止网络用户的道德风险行为。

4 结 论

由于通常的自我安全防御技术不能完全消除风险,因此网络安全保险是一种转移网络用户安全剩余风险的有效工具。理想的网络安全保险契约保证网络安全保险公司的利润,是网络安全保险市场持续发展下去的关键。本文为了改善信息非对称性对网络安全保险市场交易效率的影响,研究网络用户道德风险条件下的最优网络安全保险契约模型,使用委托代理理论建立了此类最优保险契约分析模型并对其性质进行了讨论。本文的研究结果表明:不存在网络用户道德风险时,最优网络安全保险契约可以实现风险分担的帕累托最优并要求完全保险;存在网络用户道德风险时,最优网络安全保险契约不能达到风险分担的帕累托最优和要求部分保险。

本文的局限性是假设网络中的所有用户完全相同,没有涉及网络用户异质性问题,另外,本文工作关注在信息不对称性中的道德风险问题,未来将开展网络用户逆向选择条件下的最优网络安全保险契约模型研究。

参考文献

[1] 顾建强, 梅姝娥, 仲伟俊. 基于网络安全保险的信息系统安全投资激励机制. 系统工程理论与实践, 2015, 35(4): 1057-1062

[2] Shim W. An analysis of information security management strategies in the presence of interdependent security risk. *Asia Pacific Journal of Information Systems*, 2012, 22(1):79-101

[3] 张维迎. 博弈论与信息经济学. 上海:格致出版社, 2012. 410-431

[4] 陈利华. 非对称信息下的供应链协调研究:[硕士学位论文]. 济南:山东师范大学管理与经济学院, 2010. 12-20

[5] Lelarge M, Bolot J. Cyber insurance as an incentive for internet security. In: Workshop on the Economics of Information Security, Hanover, USA, 2008. 269-290

[6] Lelarge M, Bolot J. Economic incentives to increase security in the internet: the case for insurance. In: Proceedings of the 28th International Conference on Computer

Communications, Rio de Janeiro, Brazil, 2009. 1494-502

[7] Toregas C, Zahn N. Insurance for Cyber-attacks: the issue of setting premiums in context, GW-CSPRI-2014-1. Washington: Cyber Security Policy & Research Institute, George Washington University, 2014

[8] Pal R, Golubchik L. Analyzing self-defense investments in the internet under cyber-insurance coverage. In: Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems, Genova, Italy, 2010. 339-47

[9] Hayel Y, Zhu Q. Attack-Aware Cyber Insurance for Risk Sharing in Computer Networks. Decision and Game Theory for Security. Springer International Publishing, 2015. 22-34

[10] Shetty N, Schwartz G, Felegyhazi M, et al. Competitive Cyber-Insurance and Internet Security. In: Proceedings of the 8th Workshop on the Economics of Information Security, London, England, 2010. 229-247

[11] Schwartz G, Shetty N, Walrand J. Why cyber-insurance contracts fail to reflect cyber-risks. In: Proceedings of the 51st Annual Allerton Conference on Communication, Control, and Computing, Monticello, USA, 2013. 781-787

[12] Pal R, Hui P. On differentiating cyber-insurance contracts a topological perspective. 2013

[13] Yang Z, Lui J C S. Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, 2014, 74(2):1-17

[14] Pal R, Golubchik L, Psounis K, et al. Will cyber-insurance improve network security? A market analysis. In: Proceedings of the 33rd IEEE Annual Conference on Computer Communications, Toronto, Canada, 2014. 235-243

[15] Pal R, Golubchik L, Psounis K, et al. Realizing efficient cyber-insurance markets via price discriminating security products. www-scf. usc. edu/ ~ rpal/TDSCR. pdf: USC

[16] Herath H, Herath T. Copula based actuarial model for pricing cyber-insurance policies. *Social Science Electronic Publishing*, 2011, 2(1): 6-20

[17] Mukhopadhyay A, Chatterjee S, Saha D, et al. Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, 2013, 56: 11-26

Model study of optimal cyber-insurance contracts under moral-hazard

Yang Yunxue[*,**], Wang Yanxia[*]

([*]CAS Key Lab of Network Data Science and Technology, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190)

([**]University of Chinese Academy of Sciences, Beijing 100049)

Abstract

In order to solve the decline of the trading efficiency of the cyber-insurance market caused by information asymmetry, the contract model study for optimal cyber-insurance under users' moral-hazard was conducted. Then, the analysis model for the optimal cyber-insurance contracts was established by using the principal-agent theory, and the properties of the contracts were discussed. The analyses prove that under non-moral hazard, the optimal cyber-insurance contract can achieve the Pareto Optimality in risk sharing while the full insurance coverage is required, and furthermore, the optimal cyber-insurance premium is equivalent to the expected loss caused by the network security incidents; under moral hazard, the optimal cyber-insurance contracts cannot achieve the Pareto Optimality in risk sharing while the partial insurance coverage is required, and furthermore the optimal cyber-insurance premium is less than the expected loss.

Key words: cyber-insurance, moral hazard, insurance contract, information asymmetry, Pareto Optimality