文章编号:1000-6788(2006)09-0043-08

我国商业银行防范网络安全风险的博弈模型

乔立新,袁爱玲,李淑霞,冯英浚
(哈尔滨工业大学管理学院,哈尔滨 150001)

摘要: 为探究骇客与商业银行的博弈信念,在分析骇客与商业银行对银行网络安全系统进行攻击与防御博弈时的成本和收益的基础上,运用信号博弈模型研究了骇客与商业银行博弈的状况.认为商业银行欲避免骇客进攻,需通过媒体将声誉维持在较高水平,使骇客相信对此银行进行攻击,所获得收益低于投入进攻的平均直接成本;理性的商业银行出于成本的考虑,会希望在提高声誉过程中所获得的边际利润与因骇客进攻而导致的银行损失相等.由此,监管当局应通过增加对商业银行网络安全情况检查的频率,增加对商业银行因网络信息安全风险导致损失情况的曝光力度等措施来迫使商业银行加大对网络安全的投入.

关键词: 商业银行;网络安全;博弈论;骇客
中图分类号: F832　　**文献标志码**: A

The Game Model for Reducing the Security Risk of Chinese Commercial Bank

QIAO Li-xin, YUAN Ai-ling, LI Shu-xia, FENG Ying-jun
(School of Management, Harbin Institute of Technology, Harbin 150001, China)

Abstract: In order to investigate the game behind the hackers and commercial banks, this paper analyzes the costs and profits about the attack and the defense of commercial banks & hackers, and studies the game status of hackers and commercial banks by signal game model. This paper figures that commercial banks should maintain its reputation at a higher level to prevent hacker's attack, and thus let the hacker to believe the profit will less than the average direct cost while making an attack. Regarding the cost, rational commercial banks may hope its marginal profit gained by the engagement in its reputation promotion equals to the banks' lose due to hacker's attack. This paper finally concluded that, the supervisor authorities should try to increase the inspection frequency about the status of commercial banks' network security, as well as increase the media exposing level about the losing status caused by network information security risk, and thus force the commercial banks to increase its investment on network security.

Key words: commercial bank; network security; game theory; hacker

1 引言

随着我国各商业银行网上业务量的迅猛增长,构筑牢固的网络安全风险防护系统日趋重要.目前国内外金融机构为防范骇客的进攻制定了各种制度和措施,如:巴塞尔银行监管委员会(2000,2001)先后发表的若干关于电子银行风险管理的原则和建议[1,2]及巴塞尔新协议(1999～2004)[3～8],我国(2002)发布的《商业银行内部控制指引》,The Sumitomo Trust & Banking Co., Ltd.(2004)为防范网络安全风险所建立的各种制度措施[9]等.此外,各国政府和学者还从技术上为解决这一问题提出了建议,如印度政府(2003)发起的"电子商务技术"计划[10],Watase, Jumpei 等学者(2004)所建立的安全功能增强的操作系统[11],Tang, Qiang

收稿日期:2005-08-21
资助项目:国家自然科学基金重点项目(70131010);哈尔滨市青年科学研究基金(2005AFXXJ41);哈尔滨市青年科学研究基金(2005AFXXJ41)

作者简介:乔立新(1967-),女,博士研究生,研究方向:商业银行管理、金融工程,E-mail:qiaolixin@sina.com;袁爱玲(1963-),女,硕士,副教授,研究方向:经济法;李淑霞,女,哈工大人文学院教师;冯英浚(1940-),男,教授,博士导师,研究方向:绩效管理、数理金融经济学.

(2003)所提出的采用 RSA 签名、Schnorr 签名和乱码技术而设计的离线电子支付系统[12]等. 而笔者认为通过研究骇客与商业银行博弈模型,可以更好地了解双方的博弈特点,为监管层和商业银行制定防范网络风险的策略提供理论依据. 因此,本文在分析骇客与商业银行对银行网络安全系统进行攻击与防御博弈时的成本和收益的基础上,运用信号博弈模型研究了骇客与商业银行博弈的状况,并由此提出我国商业银行维护网络系统安全的相关政策建议.

2 骇客与商业银行的信念及行动策略

骇客与商业银行之间是多重信号博弈. 设 S 是信号的发出者——商业银行, R 是信号的接收者——骇客. R 与 S 之间存在着明显的"信息不对称",即: S 知道其对网络安全的投入水平 θ_i,但 R 却不能准确掌握这些信息,只能根据 S 声誉的高低程度、以往被攻击记录、通过网络工具获取 S 所存在的"系统安全性漏洞"状况,来得出 S 类型的信念 $p(\theta_i)$.

双方博弈的展开一般遵循如下路径:

虚拟的参与人"自然"首先行动——选择 S 的类型,即给出 S 对网络安全的投入水平 θ_i 的先验信念(概率分布) $p(\theta_i)$,其中 $i \in [1, I]$,符合

$$\sum_{i=1}^{I} p(\theta_i) = 1. \tag{1}$$

S 根据 θ_i 先采取策略行动——向公众传递"S 注重网络系统安全性声誉的高低程度 d_j"(以下简称"声誉高低程度"). 这是因为,通常公众通过"声誉高低程度"这一信号来判定商业银行对网络信息安全系统的投入水平 θ_i,并认为 d_j 与 θ_i 成正比关系. 设银行决定在网络安全投入水平为 θ_i 时,表现为声誉 d_j 的概率分布为 $\sigma_{ij} = \{p(d_1 | \theta_i), p(d_2 | \theta_i), \cdots, p(d_J | \theta_i)\}$,符合

$$\sum_{j} p(d_j | \theta_i) = 1. \tag{2}$$

骇客 R 观测到 S 的声誉为 d_j 后,相机采取后动策略 Ak. 如果攻击好声誉的 S,则 R 的收益可能很小甚至出现亏损;攻击差声誉的 S,则 R 会获得较为丰厚的回报. 所以 R 的最优策略是:不攻击好声誉的商业银行(即 $Ak = 0$),而攻击差声誉的商业银行(即 $Ak = 1$). 假定 R 在观察到 S 的声誉程度为 d_j 后,采取进攻策略的信念为 $\mu_j = p(Ak | d_j)$, R 的攻击行动将进一步导致商业银行的声誉降低,这时 R 就会根据贝叶斯法则从商业银行类型的先验信念 $p(\theta_i)$ 得出关于商业银行类型的一个后验信念 $\tilde{p} = p(\theta_i | d_j)$. 这样, R 虽然起初没有真正了解商业银行,但经过多个阶段的试探后,会通过观察商业银行声誉高低的变化逐渐修正对商业银行类型的先验信念 $p(\theta_i)$,并相机采取最优决策行动. 若 R 根据后验信念 $\tilde{p} = p(\theta_i | d_j)$ 判定商业银行为投入程度高的银行,则骇客采取不攻击的策略,反之,采取攻击的策略.

而博弈的另一方——S 估测到自己的行动将被骇客所观察到,就会通过各种媒体传播自己声誉高的信息,使骇客望而却步,达到减少网络安全风险的目的,但是这样就会带来 S 成本的增加. 在经济利益的驱动下, S 应当根据骇客对 S 攻击的概率 μ_j,制定出自己最优的行动策略 σ_{ij},并在不断的博弈过程中,根据贝叶斯法则不断修正自己关于骇客攻击商业银行的先验信念 μ_j,相机选择行动策略 σ_{ij}.

由此可见,在 R 与 S 博弈的模型中, S 根据骇客攻击商业银行的概率 μ_j,来决定自己的行动策略 σ_{ij},而骇客则是通过对 S 声誉高低程度的了解和攻击结果来决定其对商业银行的攻击概率 μ_j. 这样商业银行的声誉高低程度就起到在骇客与商业银行之间的博弈中传递各自的行动策略信号的作用. 因此, S 与 R 间的博弈属于不完全信息动态博弈的范畴,是一种信号博弈(Signal Game). 根据顺向归纳法(forward induction)可得,由于 R 的攻击概率 μ_j 和 S 的信念 σ_{ij} 逐渐向均衡状态收敛,系统最终会达到精炼贝叶斯纳什均衡.

这样我们就可以构造一个 S 与 R 间的信号博弈模型,并对该模型做如下前提假定: ①该博弈是无限

次重复博弈;②S 与 R 都是充分的理性;③初始阶段 R 不清楚 S 类型 θ_i,仅具有 S 类型的先验信念 $p(\theta_i)$,而且 S 也不清楚 R 的攻击概率 $\mu_j = p(Ak \mid d_j)$;④第一阶段后,R 可以观察到 S 上一期的声誉高低程度,进而得出关于 S 类型的后验信念 $\tilde{p} = p(\theta_i \mid d_j)$,$S$ 也能了解 R 上一期的进攻概率 μ_{j-1};⑤R 和 S 在下一阶段都根据上一阶段得到的信息来决定下一阶段的行动;⑥R 和 S 的均衡函数取决于 R 对商业银行的攻击概率 μ_j 和 S 的信念 σ_{ij},且 R 的进攻概率 μ_j 和 S 的信念 σ_{ij} 向均衡状态收敛.

3　骇客和商业银行的成本收益分析

由于骇客与商业银行的博弈策略是基于自身效用或利润最大化的原则来进行,因此这里要分析骇客与商业银行的成本收益.

3.1　骇客 R 的成本与收益

1) 骇客的成本

①骇客攻击网络的直接成本 $\kappa(\theta_i, \sigma_{i,j}, \mu_j)$:通常它是与商业银行对网络安全系统的投入水平 θ_i 有关. 如果商业银行网络安全系统投入水平 θ_i 高,其获得的商业银行网络系统安全声誉也会高. 骇客可以在商业银行安全性声誉差时,攻击该银行,也可以在商业银行安全性声誉好时,攻击该银行. 如果骇客不攻击该银行,则攻击银行是无成本的. 可以用 $\kappa(\theta_i, \sigma_{i,j}, \mu_j)$ 表示骇客攻击网络的直接成本,其中 θ_i 为商业银行防范网络安全系统投入水平.

当商业银行网络安全系统投入水平为 θ_i 时,骇客的直接成本为:

$$\kappa(\theta_i, \sigma_{i,j}, \mu_j) = E(C \mid Ak) \times \mu_j \times p(d_j) = E(C \mid Ak) \times \mu_j \times \sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)], \tag{3}$$

其中:$E(C \mid Ak)$ 是骇客进攻时的期望直接成本;$p(d_j)$ 表示声誉为 d_j 的概率,μ_j 表示在声誉为 d_j 时进攻的概率,$\mu_j \times p(d_j)$ 为骇客进攻的概率,$\sigma_{i,j}$ 为在"商业银行网络安全系统投入水平为 θ_i"时选择发出信号"声誉 d_j"的概率,$p(\theta_i)$ 表示商业银行网络安全系统投入水平为 θ_i 的概率.

②处罚成本:包括骇客被捉到后的罚款、各种法律和行政处罚. 它与被发现的概率(可用 $p(e)$ 表示)正相关,可以表示为 $E(C) = E(C \mid e) \times p(e)$. 由于骇客的攻击行为被发现的概率极低. 因而可将其实际处罚成本视为 0.

综上所述,骇客的成本函数实际为骇客攻击网络的直接成本,即:

$$C(\theta_i, \sigma_{i,j}, \mu_j) = \kappa(\theta_i, \sigma_{i,j}, \mu_j) = E[C \mid Ak] \times \mu_j \times p(d_j) = E[C \mid Ak] \times \mu_j \times \sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)], \tag{4}$$

其中:$C(\theta_i, \sigma_{i,j}, \mu_j)$ 为当商业银行的策略为 θ_i 和 $\sigma_{i,j}$ 时骇客进攻的成本函数;$E(C \mid Ak)$ 是进攻时骇客的期望成本,$\mu_j \times \sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)]$ 为骇客进攻的概率.

2) 收益分析

骇客攻击商业银行的收益巨大. 根据美国官方统计,银行每年在网络上被偷窃的资金达 6000 万美元,"电子扒手"作案平均得手价值 25 万美元,而持枪抢劫银行只有 7500 美元. 最新发现的"网银大盗"电脑病毒致使网上银行潜在的资金威胁已上升到万亿级别. 如此巨大的收益,不法分子岂不铤而走险.

但是,骇客攻击商业银行计算机网络系统所获得的收益与商业银行防范网络安全系统投入水平 θ_i 是成反比的. 通常商业银行防范网络安全系统投入水平 θ_i 越高,骇客攻破商业银行计算机网络系统的概率 μ_j 越小,获得的收益也越低.

如果该银行被攻破,则骇客可以从该商业银行所获得的收益为:

$$h(\theta_i,\sigma_{i,j},\mu_j) = A \times p(d_j) \times \mu_j \times L_D = A \times \sum_{i=1}^{I}[\sigma_{i,j} \times p(\theta_i)] \times \mu_j \times L_D. \tag{5}$$

这里,A 是商业银行网上业务资金量,L_D 为骇客进攻所造成的损失程度.

从以上分析中得出当商业银行防范网络安全系统投入水平为 θ_i 时骇客的利润函数:

$$\begin{aligned} R(\theta_i,\sigma_{i,j},\mu_j) &= h(\theta_i,\sigma_{i,j},\mu_j) - C(\theta_i,\sigma_{i,j},\mu_j) \\ &= A \times p(d_j) \times \mu_j \times L_D - E[C \mid Ak] \times \mu_j \times p(d_j) \\ &= A \times \sum_{i=1}^{I}[\sigma_{i,j} \times p(\theta_i)] \times \mu_j \times L_D - E[C \mid Ak] \times \mu_j \times \sum_{i=1}^{I}[\sigma_{i,j} \times p(\theta_i)] \\ &= (A \times \mu_j \times L_D - E[C \mid Ak] \times \mu_j) \times \sum_{i=1}^{I}[\sigma_{i,j} \times p(\theta_i)] \end{aligned} \tag{6}$$

3.2 商业银行 S 的成本与收益分析

1) 商业银行 S 的成本分析

①骇客进攻时造成的商业银行直接经济损失 $L(\theta_i,\sigma_{i,j},\mu_j)$

骇客进攻时造成的商业银行直接经济损失实质上就是骇客的收益,即为:

$$L(\theta_i,\sigma_{i,j},\mu_j) = A \times p(d_j) \times c \times L_D = A \times \sum_{i=1}^{I}[\sigma_{i,j} \times p(\theta_i)] \times \mu_j \times L_D, \tag{7}$$

这里,A 是商业银行网上业务资金量,L_D 为骇客进攻所造成的损失程度.

②商业银行为防范网络安全风险而投入的各项系统维护成本

根据中国人民银行 2002 年 9 月 18 日公布的《商业银行内部控制指引》第八章的规定,商业银行在防范网络风险时,会增加 5 种系统维护成本:制度成本、雇员成本、检查成本、失去客户、数据备份成本. 此外,商业银行在防范网络信息安全风险时,还需要采取各种宣传策略以使其声誉为 d_j,这里将此营造声誉成本表示为 $M(\theta_i,\sigma_{i,j})$. 在上述这些商业银行防范网络安全风险的成本中,①由于监管机构很容易检查商业银行的制度建设和数据备份状况,并且这些工作是商业银行必须做但与其防范网络安全系统投入水平 θ_i 联系不大;另外即使制度需要进一步修订,其修订成本相对于其他成本而言也较低. 所以在成本函数中可以将制度成本和数据备份成本看成常数,两项合在一起用 $C1$ 表示. ②由于雇员成本、检查成本和失去客户成本都与商业银行防范网络安全系统投入水平 θ_i 相关,所以将三项合起来用函数 $H(\theta_i)$ 表示.

综合起来商业银行的成本函数为:

$$\begin{aligned} CS(\theta_i,\sigma_{i,j},\mu_j) &= L(\theta_i,\sigma_{i,j},\mu_j) + C1 + H(\theta_i) + M(\theta_i,\sigma_{i,j}) \\ &= A \times \sum_{i=1}^{I}[\sigma_{i,j} \times p(\theta_i)] \times \mu_j \times L_D + C1 + H(\theta_i) + M(\theta_i,\sigma_{i,j}) \end{aligned} \tag{8}$$

其中:$C1$ 为制度成本和数据备份成本,是一个常数;

$H(\theta_i)$ 为雇员成本、检查成本和失去客户成本;

$L(\theta_i,\sigma_{i,j})$ 为因骇客进攻造成的商业银行直接经济损失.

这里需要说明的是:通常商业银行根据骇客攻击造成的损失程度,以及骇客对商业银行进攻的概率来决定自己的网络系统安全性声誉的高低程度.

2) 收益分析

①在声誉为 d_j 时的收益. 商业银行的正常经营需要存款人、贷款人以及金融市场对其有充分的信心,如果声誉 d_j 低,或社会上存在对商业银行业务的不利传闻时,就会使客户对商业银行失去信心,进而出现挤兑等行为,使商业银行蒙受损失,甚至造成银行倒闭. 从长期来看,商业银行可以从无限次重复博弈的过程中获得高声誉的收益,这些收益的贴现值可以理解为"银行注重网络安全的声誉"价值,它与 $(\theta_i,\sigma_{i,j})$ 相关,可以用 $Vr(\theta_i,\sigma_{i,j})$ 表示它,$Vr(\theta_i,\sigma_{i,j}) \geq 0$.

②避免中央银行处罚. 为使商业银行与监管机构保持合作,对于不能按银监会等监管机构的要求建立严格内控机制的商业银行,监管机构必然会对其进行处罚,情节严重的还要追究银行及相关职员的刑事责任. 监管机构对问题商业银行的罚款金额用 F 表示,监管机构对商业银行进行检查的频率为 p,发现问题的概率为 $\Psi_1(\theta_i, p)$,$F \times p \times \Psi_1(\theta_i, p)$ 为监管机构对商业银行进行罚款的期望值(它代表在商业银行网络安全努力程度为 θ_i 时被监管机构罚款的金额),则避免监管机构罚款的期望收益为 $(1 - p \times \Psi_1(\theta_i)) \times F$.

故而,商业银行的期望收益可以表示为:

$$RS(\theta_i, \sigma_{i,j}) = (1 - p \cdot \Psi_1(\theta_i)) \times F + Vr(\theta_i, \sigma_{i,j}). \tag{9}$$

在以上分析的基础上得出商业银行的利润函数:

$$\begin{aligned} & W(\theta_i, \sigma_{i,j}, \mu_j) \\ &= RS(\theta_i, \sigma_{i,j}) - CS(\theta_i, \sigma_{i,j}, \mu_j) \\ &= (1 - p \cdot \Psi_1(\theta_i, p)) \times F + Vr(\theta_i, \sigma_{i,j}) - C1 - H(\theta_i) - A \times p(d_j) \times \mu_j \times L_D - M(\theta_i, \sigma_{i,j}) \\ &= (1 - p \cdot \Psi_1(\theta_i, p)) \times F + Vr(\theta_i, \sigma_{i,j}) - C1 - H(\theta_i) - A \times \sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)] \times \mu_j \times L_D - M(\theta_i, \sigma_{i,j}). \end{aligned} \tag{10}$$

3.3　均衡分析

根据贝叶斯法则,若骇客在 j 阶段观测到商业银行网络安全的声誉程度为 d_j,则骇客在 $j+1$ 阶段推断商业银行为网络安全投入水平为 θ_i 的银行的后验概率为:

$$\tilde{p} = p(\theta_i \mid d_j) = \frac{p(d_j \mid \theta_i) \times p(\theta_i)}{p(d_j)} = \frac{p(d_j \mid \theta_i) \times p(\theta_i)}{\sum_{i=1}^{I} [p(d_j \mid \theta_i) \times p(\theta_i)]} = \frac{\sigma_{i,j} \times p(\theta_i)}{\sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)]}. \tag{11}$$

则骇客的均衡满足:

$$\begin{aligned} & \max_{\mu_j, \theta_i, \sigma_{i,j}} \sum_{i=1}^{I} \tilde{p} \cdot R(\mu_j, \theta_i, \sigma_{i,j}) \\ &= \max_{\mu_j, \theta_i, \sigma_{i,j}} \sum_{i=1}^{I} \left[\frac{\sigma_{i,j} \times p(\theta_i)}{\sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)]} \times (A \times \mu_j \times L_D - E[C \mid Ak] \times \mu_j) \times \sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)] \right] \\ &= \max_{\mu_j, \theta_i, \sigma_{i,j}} \sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i) \times (A \times \mu_j \times L_D - E[C \mid Ak] \times \mu_j)] \\ &= \max_{\mu_j, \theta_i, \sigma_{i,j}} (A \times \mu_j \times L_D - E[C \mid Ak] \times \mu_j) \times \sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)] \end{aligned} \tag{12}$$

商业银行的均衡满足:

$$\begin{aligned} \max_{\theta_i, \sigma_{i,j}} W(\mu_j, \theta_i, \sigma_{i,j}) = \max_{\theta_i, \sigma_{i,j}} \Big\{ & (1 - p \cdot \Psi_1(\theta_i, p)) \times F + Vr(\theta_i, \sigma_{i,j}) - C1 - H(\theta_i) - \\ & A \times \sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)] \times \mu_j^* \times L_D - M(\theta_i, \sigma_{i,j}) \Big\} \end{aligned} \tag{13}$$

3.4　动态博弈模型的求解

对商业银行而言,其最优选择是:通过自己的策略,使得骇客在攻击时所获得的最大收益与不攻击时的收益一样. 即:

$$\begin{aligned} \max_{\mu_j, \theta_i, \sigma_{i,j}} \sum_{i=1}^{I} \tilde{p} \cdot R(\mu_j, \theta_i, \sigma_{i,j}) &= \max_{\mu_j, \theta_i, \sigma_{i,j}} (A \times \mu_j \times L_D - E[C \mid Ak] \times \mu_j) \times \sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)] \\ &= \max_{\mu_j, d_j} (A \times \mu_j \times L_D - E[C \mid Ak] \times \mu_j) \times p(d_j) = 0. \end{aligned} \tag{14}$$

因为有极大值存在,所以这就意味着

①(14)式的一阶条件为 0,即:

$$p(d_j)(A \times L_D - E[C|Ak]) = 0, \tag{15}$$

②
$$(A \times \mu_j \times L_D - E[C|Ak] \times \mu_j) \times p(d_j) \leq 0. \tag{16}$$

因为 $p(d_j) \in [0,1]$,所以(16)意味着

$$(A \times \mu_j \times L_D - E[C|Ak] \times \mu_j) \leq 0.$$

$$\mu_j \geq \frac{A \times L_D \times \mu_j}{E[C|Ak]} = \frac{B_d}{E[C|Ak]}. \tag{17}$$

(17)式中的分子 $A \times L_D \times \mu_j$ 是指在商业银行的声誉为 d_j 时骇客进攻造成的商业银行直接经济损失(也是此骇客进攻的收益),这里用 B_d 表示;分母 $E[C|Ak]$ 是骇客进攻时付出的期望成本. (17)表明:只有在骇客进攻获得的收益 ≥骇客攻击时付出的平均成本时,骇客才会采取攻击策略.

又因为骇客的进攻概率 $\mu_j \in [0.1]$,

由(15)可知,最优解为

$$(A \times L_D - E[C|Ak]) = 0 \Rightarrow A \times L_D = E[C|Ak]. \tag{18}$$

将(18)式两侧同乘以 μ_j^*,

$$A \times L_D \times \mu_j^* = E[C|Ak] \times \mu_j^*,$$

$$\mu_j^* = \frac{A \times L_D \times \mu_j^*}{E[C|Ak]} = \frac{B_d}{E[C|Ak]}. \tag{19}$$

将(19)式代入(13)得:

$$\max_{\theta_i,\sigma_{i,j}} W(\theta_i,\sigma_{i,j}) = \max_{\theta_i,\sigma_{i,j}} \left\{ (1 - p \cdot \Psi_1(\theta_i,p)) \times F + Vr(\theta_i,\sigma_{i,j}) - C1 - H(\theta_i) - A \times \sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)] \times \frac{B_d}{E[C|Ak]} \times L_D - M(\theta_i,\sigma_{i,j}) \right\}, \tag{20}$$

其对 $\sigma_{i,j}$ 的最优化一阶条件是:

$$\frac{\partial Vr(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} - A \times \frac{B_d}{E[C|Ak]} \times L_D - \frac{\partial M(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} = 0,$$

$$\frac{\partial Vr(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} - \frac{\partial M(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} = B_d. \tag{21}$$

此时商业银行对声誉应拥有的策略信念为:$\sigma_{i,j}^*$.

在上述假设下,博弈模型存在如下的精炼贝叶斯纳什均衡:

$$(\sigma_{i,j}^*, \mu_j^*; \tilde{p}) = \left(\sigma_{i,j}^*, \frac{B_d}{E[C|Ak]}; \frac{\sigma_{i,j} \times p(\theta_i)}{\sum_{i=1}^{I} [\sigma_{i,j} \times p(\theta_i)]} \right). \tag{22}$$

4 博弈的均衡信念分析和结论

4.1 分析骇客的均衡信念

由(17)和(19)式可得出以下结论:

当骇客了解到商业银行的策略 $\sigma_{i,j}$ 后,若骇客认为进攻的收益 = 骇客进攻时付出的平均直接成本 $E[C|Ak]$,骇客对是否选择进攻策略持无所谓态度;若骇客认为进攻的收益 > 骇客进攻时的平均直接成本 $E[C|Ak]$,骇客肯定会进攻;若骇客认为进攻的收益 < 骇客进攻时的平均直接成本 $E[C|Ak]$,骇客肯定不会采取进攻策略.

这一结论提示商业银行在制定防范网络信息安全风险的策略(决定 θ_i 和 $\sigma_{i,j}$)时,要了解骇客进攻的

平均直接成本 $E[C|Ak]$,并采取各种防护措施,使骇客的收益低于该平均直接成本.

4.2　分析商业银行的均衡信念

当商业银行相信骇客的策略信念为 μ^* 时,它的行动策略有如下选择:总是低声誉,$\sigma_{i,j}^* \equiv 0$;总是高声誉,$d_j^* \equiv 1$;混合策略,$\sigma_{i,j}^* \in [0,1]$.

1) 如果商业银行对高声誉和低声誉选择持无所谓态度(风险中性者),$\sigma_{i,j}^* \in [0,1]$,则等价于:

$$\frac{\partial Vr(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} - \frac{\partial M(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} = B_d, \tag{23}$$

这意味着:商业银行在采取各种措施提高声誉 $\sigma_{i,j}$ 的过程中所获的边际利润 $\left(\frac{\partial Vr(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} - \frac{\partial M(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}}\right)$ 与骇客进攻的收益 B_d 相等.

2) 如果商业银行总是选择高声誉,$\sigma_{i,j}^* \equiv 1$,则等价于:

$$\frac{\partial Vr(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} - \frac{\partial M(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} > B_d, \tag{24}$$

这意味着:高声誉商业银行在采取各种措施提高声誉 $\sigma_{i,j}$ 的过程中所获的边际利润 $\left(\frac{\partial Vr(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} - \frac{\partial M(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}}\right)$ 大于骇客进攻的收益 B_d. 说明始终维持高声誉的商业银行,在同骇客的长期信号博弈过程中,最终会减少因骇客进攻而导致的网络信息安全风险损失,此时骇客进攻的策略信念应为 $\mu < \mu^*$.

3) 如果商业银行总是选择低声誉,$\sigma_{i,j}^* \equiv 0$,则等价于:

$$\frac{\partial Vr(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} - \frac{\partial M(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} < B_d, \tag{25}$$

这意味着:低声誉商业银行从维持声誉 $\sigma_{i,j}$ 中所获的边际利润 $\left(\frac{\partial Vr(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} - \frac{\partial M(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}}\right)$ 要小于骇客进攻的收益 B_d. 说明通过长期的信号博弈,低声誉的商业银行受到骇客进攻的概率大($\mu > \mu^*$),因骇客进攻而导致的网络信息安全风险损失程度严重.

由对骇客和商业银行均衡信念的分析,可以得出以下策略启示:

1) 可以说,目前任何网络防护措施都不完善,对于某些骇客来说甚至形同虚设,所以商业银行若要避免骇客进攻,就需要通过媒体将声誉 $\sigma_{i,j}$ 维持在某一较高水平,使骇客相信对这种声誉的商业银行进行攻击,所获得的收益要低于投入进攻的平均直接成本 $E[C|Ak]$,从而达到用高声誉震慑骇客的目的. 具体而言,若商业银行认为骇客的策略信念为 μ^*,它采取的最优策略是将声誉设为 $\sigma_{i,j}^*$;若商业银行认为骇客的策略信念为 $\mu > \mu^*$,商业银行必须要采取各种措施制造高声誉来诱使骇客放弃攻击行动;若商业银行认为骇客的策略信念为 $\mu < \mu^*$,商业银行维持现有声誉即可.

2) 理性的商业银行出于成本的考虑,会希望在提高声誉 $\sigma_{i,j}$ 过程中所获得的边际利润 $\left(\frac{\partial Vr(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}} - \frac{\partial M(\theta_i,\sigma_{i,j})}{\partial \sigma_{i,j}}\right)$ 与骇客进攻的收益 B_d 相等. 由于很难预测骇客进攻的收益 B_d(即商业银行的损失)有多大,而且目前中国各家商业银行的网上业务都还不是它的主要利润来源,所以出于对网络安全投入成本较其它业务要高的考虑,各家商业银行都不会有积极性去加大对网络安全的投入水平,这就需要监管当局通过相应的制度来迫使商业银行加大对网络安全的投入水平,其中最有效的措施之一就是监管当局增加对商业银行网络安全情况检查的频率,以督促商业银行加大对网络信息安全的投入,从而保证商业银行网络信息系统的安全;另一有效措施是增加对商业银行因网络信息安全风险导致损失情况的曝光力度,以警示各家商业银行"网络安全风险是一种损失程度巨大的操作风险损失事件类型",提高各家银行对它的重视程度.

参考文献:

[1] Basel Committee on Banking Supervision. Risk Management Principles for Electronic Banking [DB/OL]. http:// www. bis. org, May 2001.

[2] Basel Committee on Banking Supervision. Electronic Banking Group Initiatives and White Papers [DB/OL]. http://www. bis. org, October 2000.

[3] Basle Committee on Banking Supervision. Operational Risk Management [DB/OL]. http://www. bis. org, September 1998.

[4] Basle Committee on Banking Supervision. Consultative Document: Operational Risk [DB/OL]. http://www. bis. org, Jan, 2001.

[5] Basle Committee on Banking Supervision. Sound Practices for the Management and Supervision of Operational Risk [DB/OL]. http://www. bis. org, December, 2001.

[6] Basle Committee on Banking Supervision. Sound Practices for the Management and Supervision of Operational Risk [DB/OL]. http://www. bis. org, July, 2002.

[7] Basle Committee on Banking Supervision. Sound Practices for the Management and Supervision of Operational Risk [DB/OL]. http://www. bis. org, Feb, 2003.

[8] Basle Committee on Banking Supervision. Basel Ⅱ: International Convergence of Capital Measurement and Capital Standards: a Revised Framework [DB/OL]. http://www. bis. org/publ/bcbs107. htm, 2004. 7. 5.

[9] The Sumitomo Trust & Banking Co., Ltd. 2004 Annual Report - Risk Management Structure [DB/OL]. http://www. sumitomotrust. co. jp/IR/company/jp/pdf/an2004/14. pdf, 2004:36 - 45.

[10] Saxena, Ashutosh, Dani A R. Technologies for E-commerce: India initiatives [C]//IEEE Region 10 Annual International Conference, Proceedings/TENCON, 2003, (4):1434 - 1438.

[11] Jumpei W, Yoichi H, Itoh Mitsutaka. OS with enhanced security functions for protecting information systems against unauthorized access, viruses, and worms[J]. NTT Technical Review, 2004, 2, (6): 56 - 60.

[12] Tang Qiang. A new divisible anonymous off-line electronic payment system[C]//Proceedings of the IASTED International Conference on Communication, Network, and Information Security, 2003:103 - 107.