基于 Gordon-Loeb 模型的信息安全投资博弈研究

王秦，朱建明
（中央财经大学信息学院，北京 100081）

摘 要：为了研究信息安全投资外部性的影响，将 Gordon-Loeb 模型扩展到多组织博弈环境下，分别得出在正负外部性下，面对不同类型的攻击时，最优信息安全投资与脆弱性、潜在损失和投资效率的关系，并且比较了与社会最优条件下最优信息安全投资的差别。结果表明，正外部性条件下的信息安全投资变化规律与单一组织的情况相比存在一定相似之处，但负外部性下的信息安全投资改变较大，总体更加谨慎，并且攻击类型对于信息安全投资有着重要影响。

关键词：信息安全投资；Gordon-Loeb 模型；外部性；攻击类型
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018027

Research on the game of information security investment based on the Gordon-Loeb model

WANG Qin, ZHU Jianming
School of Information, Central University of Finance and Economics, Beijing 100081, China

Abstract: In order to study the impacts of externalities of information security investment, the Gordon-Loeb model was extended to a multi-organization game environment. The relationships of the optimal information security investment with vulnerability, potential loss and investment effectiveness when confronted with different attack types under the positive and negative externalities were obtained respectively, and the difference with the optimal information security investment under the social optimum condition was compared. The results show that there were some similarities in the varying pattern of information security investment between the condition of the positive externality and a single organization, but information security investment under the negative externality changes greatly and was generally more cautious, and attack types also have important impacts on information security investment.

Key words: information security investment, Gordon-Loeb model, externality, attack type

1 引言

网络时代计算机系统的互联方便了信息的传播，但也使信息安全漏洞更加难以防范。业务上相互有来往的组织，特别是关系密切的组织往往会建立便捷的沟通渠道，甚至在这些渠道上没有进行信息加密等防护手段。攻击者可以通过被劫持的主机向与其相连的主机发起攻击，也能轻易地从安全性较高的攻击目标转移到安全性较低的个体上。信息安全投资决定了组织的安全水平，在网络互连的情况下，组织的安全水平会互相影响，因此，信息安全投资具有显著的外部性，进行投资时必须考虑主体间相互联系的特点。另一方面，不同类型的攻击，如拒绝服务攻击、病毒、木马等发生概率和产生的

收稿日期：2017-09-13；**修回日期**：2018-01-02
基金项目：国家重点研发计划基金资助项目（No.2017YFB1400700）；国家自然科学基金资助项目（No.U1509214, No.61272398）
Foundation Items: The National Key R&D Program of China (No.2017YFB1400700), The National Natural Science Foundation of China (No.U1509214, No.61272398)

损失差别很大，进行信息安全投资必须考虑攻击的特点。

由于传统的技术手段难以准确适用于信息安全投资的分析[1]，Gordon 等[2]于 2002 年率先提出了使用经济学方法分析最优信息安全投资额的 Gordon-Loeb 模型。Gordon-Loeb 模型使用收益最大化原理分析了最优信息安全投资量及其特点，通过对 2 种典型的漏洞概率函数的分析，推测最优信息安全量少于攻击带来的预期损失的$\frac{1}{\mathrm{e}}$（$\frac{1}{\mathrm{e}}$定律），并不一定随着系统脆弱性的增大而提高。由于 Gordon-Loeb 模型研究的是单一组织、单一威胁的情形，形式较为简单，然后有许多研究试图对这一经典模型进行扩展。陈天平等[3]研究了如何结合效用理论制定信息安全投资方案。Gordon 等[4]加入了对外部性的考量。Huang 等[5]分析了在面对多个外部实体同时攻击时的最优信息安全投资量，在文献[6]中结合效用理论分析风险厌恶决策者的信息安全投资行为，并讨论最优信息安全额与脆弱性、风险厌恶程度等变量的关系。Huang 等[7]基于 Gordon-Loeb 模型分析在医疗信息交换中的最优信息安全投资量，并考虑网络特点的影响。

然而，以上研究或是针对单一组织的研究，或虽然研究的是多个组织互相影响的情况，但没有使用博弈论方法，无法分析组织间复杂的策略互动。在现有的基于 Gordon-Loeb 模型的博弈研究中，Gordon 等[8]基于 Gordon-Loeb 模型分析了信息共享的效应，假设其他组织的信息安全投资可以对本组织的投资起到一定的补充作用，主要从社会福利的角度进行分析，并没有深入探讨外部性的影响。巩国权等[9]研究了双寡头垄断竞争条件下信息安全投资如何影响市场需求和企业利润，但并没有考虑最优信息安全投资与脆弱性、潜在损失等关键变量的关系。Lelarge[10]基于 Gordon-Loeb 模型分析网络用户的动机协调问题，研究重点在于如何获得信息安全投资的单调性条件以及如何确保各主体达到更高的安全水平。Wu 等[11]基于 Gordon-Loeb 模型分析了在考虑攻击类型和网络脆弱性时的信息安全投资博弈模型，然而并没有考虑到信息安全投资的负外部性，也没有考虑损失的可叠加程度以及最优投资与投资效率的关系。

对于信息安全投资的研究除了主流的与 Gordon-Loeb 模型相关的文献外，还包括少数单独基于博弈论[12]、效用理论[13] 和财务分析[14]等方法的研究。然而，以上文献的共同缺点是缺乏在外部性环境中对于最优信息安全投资与安全属性关系的研究。本文将 Gordon-Loeb 模型移植到相互影响的组织间的信息安全投资问题上，使用博弈论刻画投资的外部性，考虑不同的攻击类型。本文重点回答了在组织相互依赖的条件下最优信息安全投资额如何随潜在损失、脆弱性和投资效率等参数变化，旨在得出不同的外部性对信息安全投资规律的影响，并加深关于攻击类型对信息安全投资影响的理解。

2　Gordon-Loeb 模型及信息安全投资的外部性

2.1　Gordon-Loeb 模型及其假设

Gordon-Loeb 模型研究了风险中立组织如何得出用于保护某一信息集的最优信息安全投资额，以及脆弱性、潜在损失与最优信息安全投资额的关系[2]。Gordon-Loeb 模型指出，最优信息安全投资随潜在损失的增大而提高，并且在潜在损失给定的情况下，组织不一定必须将投资集中于高脆弱性的信息集上，因为此时保护该信息集的代价过大，组织应该重点保护中等脆弱性的信息集，并且，根据文中给出的 2 种漏洞概率函数，最优信息安全投资额远远小于没有信息安全投资时的预期损失。

Gordon-Loeb 模型考虑的是单一阶段、单一事件的信息安全投资模型。需要被保护的信息集由 3 个参数，即为 t、v 和 L。其中，t 为组织受到的外在威胁（$0<t<1$），即受到攻击的概率，v 为该信息集的脆弱性（$0<v<1$），L 表示以金钱计量的被攻破后遭受的损失（$L>0$），v 反映了信息集的固有属性，不受信息安全投资影响，只能通过增加或减少访问入口等措施改变。v 值越大表示信息集的安全程度越低。假设 w 表示以金钱计量的信息安全投资额，包括购置与信息安全相关的软硬件以及人员培训等费用。信息集被攻破的概率，即安全漏洞概率函数 S 为 t、v 和 w 的函数。安全漏洞概率函数 $S(t,v,w)$必须满足

$$S(t,0,w)=0 \tag{1}$$

$$S(t,v,0)=tv \tag{2}$$

$$\frac{\partial S(t,v,w)}{\partial w}\leqslant 0 \tag{3}$$

$$\frac{\partial S^2(t,v,w)}{\partial w^2} \geqslant 0 \tag{4}$$

$$\lim_{w\to+\infty} S(t,v,w) = 0 \tag{5}$$

式(1)说明当 v=0 时，信息集将处于绝对安全的状态，此时无论外在威胁和信息安全投资为何值，攻击都必将失败。式(2)说明当信息安全投资 w=0 时，漏洞风险应当等于外在威胁与脆弱性的乘积。式(3)和式(4)说明漏洞风险随信息安全投资以递减的速度下降，即信息安全投资必须符合边际报酬递减规律。式(5)说明不断增长的信息安全投资最终能够将安全风险降至接近于 0。

不同的漏洞概率函数代表不同的攻击类型。Gordon-Loeb 模型中使用的漏洞概率函数主要包含 2 种类型，分别为目标攻击和机会攻击。

$$S^{\mathrm{I}}(t^{\mathrm{I}},v,w^{\mathrm{I}}) = \frac{t^{\mathrm{I}}v}{kw^{\mathrm{I}}+1} \tag{6}$$

$$S^{\mathrm{II}}(t^{\mathrm{II}},v,w^{\mathrm{II}}) = t^{\mathrm{II}}v^{kw^{\mathrm{II}}+1} \tag{7}$$

其中，k 表示投资效率，衡量信息安全投资能在何种程度上降低安全风险，有 $k>0$。式(6)代表目标攻击，即攻击只针对少量对象，但可能造成较大伤害，例如，针对特定用户的信息盗用。式(7)代表机会攻击，即攻击并不针对特定个体，而以大规模方式展开，例如，通过计算机病毒感染发起的攻击。2 种漏洞概率函数均与外在威胁呈线性相关关系，表示受到攻击的概率在组织可控范围之外。图 1 和图 2 分别描述了当其他参数相等时，在目标攻击和机会攻击下漏洞概率函数随脆弱性和信息安全投资的变化情况。

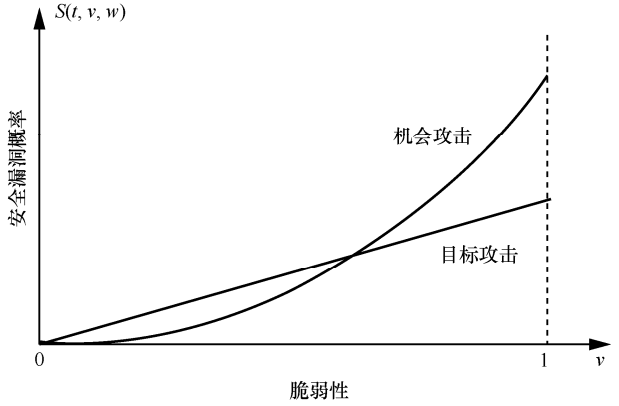

图 1 漏洞风险与脆弱性的关系

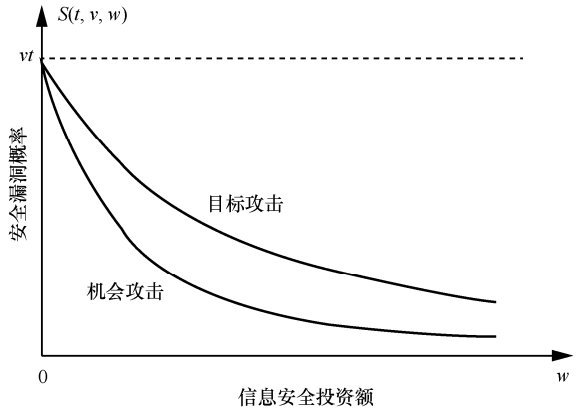

图 2 漏洞风险与信息安全投资额的关系

从图 1 可以看出，对于目标攻击，漏洞风险随脆弱性线性增长；对于机会攻击，当脆弱性较小时，漏洞风险随脆弱性增长较慢，而高脆弱性对漏洞概率函数的影响很大，这也反映出高脆弱性信息集很难抵御机会攻击的事实。从图 2 可以看出，在外在威胁以及脆弱性相等的情况下，等量的信息安全投资对于机会攻击的抵御效果更好，显示目标攻击相较机会攻击更难防范。

2.2 信息安全投资的外部性

在网络环境下，组织的信息安全投资会不可避免地相互影响，产生溢出效应。信息安全投资的外部性可以分为正外部性和负外部性。

当信息安全投资的外部性表现为正外部性时，组织可以从其他组织的信息安全投资中获得好处。一方信息安全投资的增加，不仅会使自身安全程度提高，还会使与之直接或间接相连的组织安全程度增加。假设包含 2 个组织的情况，此时，组织存在 2 种遭受信息安全攻击的途径，即直接入侵和间接入侵。直接入侵是指由于组织自身的脆弱性招致的入侵，间接入侵是指攻击者通过攻入与该组织相连的其他组织进而入侵该组织。假设组织 1 和组织 2 之间相互感染的概率为 q。q 衡量了组织间相互联系的紧密程度，有 $0<q<1$。设 a 表示直接入侵和间接入侵可以相互叠加的程度，当 $a=0$ 时，入侵可以叠加，即组织可以同时遭受 2 种入侵，当 $a=1$ 时，入侵不可叠加。组织 1 的信息集被攻破的概率为

$$p_1(w_1,w_2) = S_1(w_1) + [1-aS_1(w_1)]qS_2(w_2) \tag{8}$$

其中，w_1 和 w_2 分别是组织 1 和组织 2 的信息安全投资，S_1 和 S_2 分别是组织 1 和组织 2 的安全漏洞概率函数。$S_1(w_1)$ 为组织 1 被直接入侵的概率，$[1-aS_1(w_1)]qS_2(w_2)$ 为组织 1 被间接入侵的概率。由

式(8)可知 $\frac{\partial p_1(w_1,w_2)}{\partial w_1}<0$，$\frac{\partial p_1(w_1,w_2)}{\partial w_2}<0$，即组织 2 的信息安全投资有助于降低组织 1 的安全漏洞概率。组织 2 的信息集被攻破的概率表达式可以以此类推。

在多数现实情况中，信息安全投资外部性的表现以正外部性为主。然而，有时信息安全投资会呈现负外部性，此时，攻击者无法通过组织间的联系实现间接入侵，并且当某一组织的信息安全投资增加时，其安全程度的提高会促使攻击者将目标转移到安全程度更低的组织上，因此，更多的信息安全投资反而对其他组织有害。假设在包含 2 个组织的情况下，当信息安全投资出现负外部性时，组织 1 的信息集被攻破的概率为

$$p_1(w_1,w_2)=S_1(w_1\mathrm{e}^{w_1-w_2}) \tag{9}$$

由式(9)可知 $\frac{\partial p_1(w_1,w_2)}{\partial w_1}<0$，$\frac{\partial p_1(w_1,w_2)}{\partial w_2}>0$，即组织 2 的信息安全投资会增大组织 1 的信息集被攻破的概率。当 $w_1=w_2$ 时，组织 1 的信息安全投资不受影响，相当于不存在外部性的情况。当 $w_2>w_1$ 时，组织 2 的信息安全投资超过了组织 1，会吸引更多的攻击者转向组织 1，相当于削弱了组织 1 的信息安全投资。相反，当 $w_2<w_1$ 时，更多的攻击者会转向组织 2，相当于增加了组织 1 的信息安全投资。

3　基于 Gordon-Loeb 模型的博弈模型构建

假设博弈在 2 个同质的参与方之间展开，即组织 1 和组织 2 面临的外在威胁 t、脆弱性 v、预期损失 L 和投资效率 k 相等。博弈同时在进行。组织 1 和组织 2 在考虑对方信息安全投资的情况下，选择信息安全投资额以最大化其净收益。2 个组织之间的博弈关系如图 3 所示。

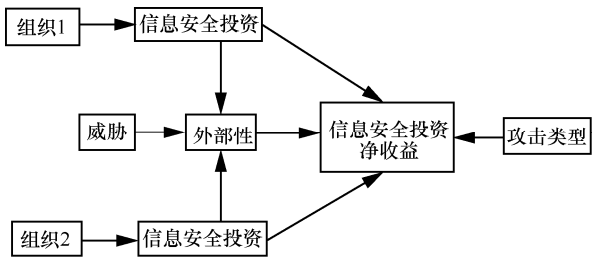

图 3　组织信息安全投资博弈关系

组织 1 的净收益为信息安全投资的预期收益减去成本，即

$$E_1(w_1,w_2)=[tv-p_1(w_1,w_2)]L-w_1 \tag{10}$$

其中，tv 为不进行信息安全投资时的安全漏洞概率，$[tv-p_1(w_1,w_2)]L$ 为信息安全投资带来的预期损失的减少，即信息安全投资的预期收益，w_1 可以看作组织的信息安全投资成本。

组织 1 的最优信息安全投资的一阶条件为

$$-\frac{\partial p_1(w_1,w_2)}{\partial w_1}L-1=0 \tag{11}$$

$-\frac{\partial p_1(w_1,w_2)}{\partial w_1}L$ 可以看作信息安全投资的单位收益，1 可以看作信息安全投资的单位成本。组织进行信息安全投资的目标是使其单位收益与单位成本相等。

由式(11)可知，对于正外部性的情况，一阶条件为

$$-[S_1'(w_1)-aqS_1'(w_1)S_2(w_2)]L-1=0 \tag{12}$$

对于负外部性的情况，一阶条件为

$$-(\mathrm{e}^{w_1-w_2}+w_1\mathrm{e}^{w_1-w_2})S_1'(w_1\mathrm{e}^{w_1-w_2})L-1=0 \tag{13}$$

该一阶条件也是组织 1 对组织 2 的反应曲线。同理可得组织 2 对组织 1 的反应曲线。为了保证纳什均衡的存在，必须有

$$\frac{\partial w_2}{\partial w_1}>\frac{\partial w_1}{\partial w_2} \tag{14}$$

在纳什均衡下，由于 2 个组织是同质的，根据对称性，必有

$$w_1^*=w_2^*=w^* \tag{15}$$

信息安全投资规律要受外部性和攻击类型的制约。接着，分别讨论在正外部性和负外部性下对不同类型的攻击时，最优信息安全投资随潜在损失、脆弱性和投资效率的变化情况。

4　正外部性下的最优信息安全投资

为了方便区分，使用 w_p^* 表示正外部性下的最优信息安全投资，使用 w_n^* 表示负外部性下的最优信息安全投资。根据式(6)、式(7)、式(12)和式(14)，在 2 个组织之间呈现正外部性的情况下，为保证纳什均衡的存在，面对目标攻击和机会攻击时分别必须满足

$$\frac{2(kw_p^{\mathrm{I}*}+1-aqvt^{\mathrm{I}})}{aqvt^{\mathrm{I}}}>\frac{aqvt^{\mathrm{I}}}{2(kw_p^{\mathrm{I}*}+1-aqvt^{\mathrm{I}})} \tag{16}$$

$$\frac{1-aqvt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}}{aqvt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}}>\frac{aqvt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}}{1-aqvt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}} \tag{17}$$

因此，可得

$$3aqvt^{\mathrm{I}} < 2(kw_p^{\mathrm{I}*}+1) \tag{18}$$

$$2aqv^{kw_p^{\mathrm{II}*}+1}t^{\mathrm{II}} < 1 \tag{19}$$

根据式(12)和式(15)，在 2 个组织之间呈现正外部性时，纳什均衡解 w_p^* 满足

$$-[S'(w_p^*)-aqS'(w_p^*)S(w_p^*)]L-1=0 \tag{20}$$

因此，对于目标攻击和机会攻击分别必须满足

$$-\frac{kvt^{\mathrm{I}}}{(kw_p^{\mathrm{I}*}+1)^2}\left(1-aq\frac{vt^{\mathrm{I}}}{kw_p^{\mathrm{I}*}+1}\right)L^{\mathrm{I}}+1=0 \tag{21}$$

$$k(\ln v)t^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}(1-aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1})L^{\mathrm{II}}+1=0 \tag{22}$$

由于 w_p^* 的具体形式难以求得，本文令 $F=-\frac{kvt^{\mathrm{I}}}{(kw_p^{\mathrm{I}*}+1)^2}\left(1-aq\frac{vt^{\mathrm{I}}}{kw_p^{\mathrm{I}*}+1}\right)L^{\mathrm{I}}+1=0$ 以及 $F=k(\ln v)t^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}(1-aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1})L^{\mathrm{II}}+1=0$，通过使用隐函数求导法则，即 $\frac{\mathrm{d}y}{\mathrm{d}x}=-\frac{\frac{\partial F}{\partial x}}{\frac{\partial F}{\partial y}}$，来确定最优信息安全投资与潜在损失、脆弱性以及投资效率的关系。

4.1 正外部性下的最优信息安全投资与潜在损失

分别对式(21)和式(22)应用隐函数的求导法则，可得

$$\frac{\partial w_p^{\mathrm{I}*}}{\partial L^{\mathrm{I}}}=\frac{(kw_p^{\mathrm{I}*}+1)(kw_p^{\mathrm{I}*}+1-aqvt^{\mathrm{I}})}{kL^{\mathrm{I}}(2kw_p^{\mathrm{I}*}+2-3aqvt^{\mathrm{I}})} \tag{23}$$

$$\frac{\partial w_p^{\mathrm{II}*}}{\partial L^{\mathrm{II}}}=\frac{1-aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}}{k(\ln v)L^{\mathrm{II}}(2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}-1)} \tag{24}$$

根据式(18)和式(19)，有

$$\frac{\partial w_p^{\mathrm{I}*}}{\partial L^{\mathrm{I}}}>0 \tag{25}$$

$$\frac{\partial w_p^{\mathrm{II}*}}{\partial L^{\mathrm{II}}}>0 \tag{26}$$

因此，可得到以下定理。

定理 1 在相互博弈的 2 个组织之间呈现正外部性的情况下，面对目标攻击和机会攻击时最优信息安全投资与潜在损失呈正相关关系。

总体而言，无论面对目标攻击还是机会攻击，最优信息安全投资额必须随潜在损失的增大而增长，以控制安全漏洞发生的概率，平衡安全漏洞带来的预期损失，这一点与 Gordon-Loeb 模型的结论一致。此外，从式(23)和式(24)可以看出，当潜在损失趋近于正无穷时，$\frac{\partial w_p^{\mathrm{I}*}}{\partial L^{\mathrm{I}}}$ 和 $\frac{\partial w_p^{\mathrm{II}*}}{\partial L^{\mathrm{II}}}$ 趋近于 0。当相互联系的组织间表现出正外部性时，虽然其他组织的信息安全投资有助于降低本组织安全漏洞发生的总体概率，然而与单一组织的情况相比，组织不仅要承受直接入侵的损失，还要承受间接入侵的损失。当潜在损失无限增大时，组织向信息安全投入更多资源开始变得于事无补，需要逐渐停止新增信息安全投资。

4.2 正外部性下的最优信息安全投资与脆弱性

同理，应用隐函数的求导法则可得

$$\frac{\partial w_p^{\mathrm{I}*}}{\partial v}=\frac{(kw_p^{\mathrm{I}*}+1)(kw_p^{\mathrm{I}*}+1-2aqvt^{\mathrm{I}})}{kv(2kw_p^{\mathrm{I}*}+2-3aqvt^{\mathrm{I}})} \tag{27}$$

$$\frac{\partial w_p^{\mathrm{II}*}}{\partial v}=\frac{(kw_p^{\mathrm{II}*}+1)(\ln v)(1-2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1})+1-aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}}{kv(\ln v)^2(2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}-1)} \tag{28}$$

根据式(18)和式(19)，有 $kv(2kw_p^{\mathrm{I}*}+2-3aqvt^{\mathrm{I}})>0$，$kv(\ln v)^2(2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}-1)<0$。当 v 趋近于 0 时，$(kw_p^{\mathrm{I}*}+1)(kw_p^{\mathrm{I}*}+1-2aqvt^{\mathrm{I}})>0$，$(kw_p^{\mathrm{II}*}+1)(\ln v)(1-2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1})+1-aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}<0$；当 v 趋近于 1 时，$(kw_p^{\mathrm{II}*}+1)(\ln v)(1-2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1})+1-aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}>0$，若 aqt^{I} 较小，则 $(kw_p^{\mathrm{I}*}+1)(kw_p^{\mathrm{I}*}+1-2aqvt^{\mathrm{I}})<0$，否则，$(kw_p^{\mathrm{I}*}+1)(kw_p^{\mathrm{I}*}+1-2aqvt^{\mathrm{I}})>0$。

因此，可得到以下定理。

定理 2 在相互博弈的 2 个组织之间呈现正外部性的情况下，当面对机会攻击时，最优信息安全投资随脆弱性的提高先增大后减小；当面对目标攻击时，若入侵的可叠加程度、感染概率以及外在威胁较小，则最优信息安全投资始终随脆弱性的提高而增大，反之，若入侵的可叠加程度、感染概率以及外在威胁较大，则最优信息安全投资随脆弱性的提高先增大后减小。

面对机会攻击和目标攻击时，最优信息安全投资与脆弱性关系的表现并不相同。机会攻击相比目标攻击，其攻击以大规模、随机化为特点，当信息集的脆弱性较低时，攻击较易被抵御，少量的信息安全投资即能起到很好的效果。然而，当脆弱性大于一定值时，机会攻击将变得很难被抵御。组织进

行信息安全投资需要平衡考虑收益与成本。过大的脆弱性使新增的安全投资难以将安全漏洞概率降低到一定程度，反而会带来成本的提高，因此，组织将选择不再增加安全投资。目标攻击只针对某些对象，并且造成的伤害较大，若入侵的可叠加程度、感染概率以及外在威胁较小，组织必须随着脆弱性的升高持续增加信息安全投资。若入侵的可叠加程度、感染概率以及外在威胁较大，在高脆弱性下新增信息安全投资同样将变得不划算。

由此可见，在博弈环境下，组织在面对机会攻击和目标攻击时同样都会出现信息安全投资随脆弱性下降的情况。组织有必要对所处环境进行详细分析，准确判断攻击类型以及信息安全投资随脆弱性变化的临界点。当脆弱性较大时，组织应考虑将重点转移到如何降低被攻破后的损失上，并在后续工作中努力降低信息集的脆弱性。

4.3　正外部性下的最优信息安全投资与投资效率

之前的研究均假设信息安全投资能够顺利展开，有效降低安全风险。然而由于客观因素的限制，现实中信息安全投资往往呈现出不同的投资效率。本节将研究投资效率对最优信息安全投资的影响。

分别对式(21)和式(22)应用隐函数的求导法则，可得

$$\frac{\partial w_p^{\mathrm{I}*}}{\partial k}=\frac{(kw_p^{\mathrm{I}*}+1)(kw_p^{\mathrm{I}*}+1-aqvt^{\mathrm{I}})}{k^2L^{\mathrm{I}}(2kw_p^{\mathrm{I}*}+2-3aqvt^{\mathrm{I}})} \tag{29}$$

$$\frac{\partial w_p^{\mathrm{II}*}}{\partial k}=\frac{1-aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}+kw_p^{\mathrm{II}*}(\ln v)(1-2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1})}{k^2(\ln v)(2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}-1)} \tag{30}$$

根据式(18)和式(19)，有

$$\frac{\partial w_p^{\mathrm{I}*}}{\partial k}>0$$

$$k^2(\ln v)(2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}-1)>0 \tag{31}$$

当 k 趋近 0 时，$1-aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}+kw_p^{\mathrm{II}*}(\ln v)(1-2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1})>0$，当 k 较大时，$1-aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1}+kw_p^{\mathrm{II}*}(\ln v)(1-2aqt^{\mathrm{II}}v^{kw_p^{\mathrm{II}*}+1})<0$。

因此，可得到以下定理。

定理 3　在相互博弈的 2 个组织之间呈现正外部性的情况下，当面对目标攻击时，最优信息安全投资随投资效率的提高而增大；当面对机会攻击时，最优信息安全投资随投资效率的提高先增大后减小。

当投资效率较小时，为了更好地抵御攻击，伴随着不断增长的投资效率，组织需要持续追加信息安全投资。当投资效率超过一定临界点，对于目标攻击，由于其更难被抵御的特点，组织仍需继续增加投资，而对于机会攻击，由于信息安全投资对其的防御效果更好，并且投资对安全风险的降低作用一直处于不断下降的趋势，因此，在高投资效率下组织将选择不再追加信息安全投资。

5　负外部性下的最优信息安全投资

根据式(6)、式(7)、式(13)和式(14)，在 2 个组织之间呈现负外部性的情况下，为保证纳什均衡的存在，面对目标攻击和机会攻击时分别必须满足

$$\frac{2(kw_n^{\mathrm{I}*}+1)(w_n^{\mathrm{I}*}+1)-(w_n^{\mathrm{I}*}+2)vt^{\mathrm{I}}L^{\mathrm{I}}}{2(kw_n^{\mathrm{I}*}+1)w_n^{\mathrm{I}*}-(w_n^{\mathrm{I}*}+1)vt^{\mathrm{I}}L^{\mathrm{I}}}>\frac{2(kw_n^{\mathrm{I}*}+1)w_n^{\mathrm{I}*}-(w_n^{\mathrm{I}*}+1)vt^{\mathrm{I}}L^{\mathrm{I}}}{2(kw_n^{\mathrm{I}*}+1)(w_n^{\mathrm{I}*}+1)-(w_n^{\mathrm{I}*}+2)vt^{\mathrm{I}}L^{\mathrm{I}}} \tag{32}$$

$$\frac{2+w_n^{\mathrm{II}*}+(1+w_n^{\mathrm{II}*})^2k(\ln v)}{1+w_n^{\mathrm{II}*}+(1+w_n^{\mathrm{II}*})w_n^{\mathrm{II}*}k(\ln v)}>\frac{1+w_n^{\mathrm{II}*}+(1+w_n^{\mathrm{II}*})w_n^{\mathrm{II}*}k(\ln v)}{2+w_n^{\mathrm{II}*}+(1+w_n^{\mathrm{II}*})^2k(\ln v)} \tag{33}$$

因此，可得

$$vt^{\mathrm{I}}L^{\mathrm{I}}>2(kw_n^{\mathrm{I}*}+1) \tag{34}$$

$$k(\ln v)>-\frac{1}{w_n^{\mathrm{II}*}+1} \tag{35}$$

根据式(13)和式(15)，在 2 个组织之间呈现负外部性时，纳什均衡解 w_n^* 满足

$$-(1+w_n^*)S'(w_n^*)L-1=0 \tag{36}$$

因此，对于目标攻击和机会攻击分别必须满足

$$(1+w_n^{\mathrm{I}*})\frac{kvt^{\mathrm{I}}}{(kw_n^{\mathrm{I}*}+1)^2}-1=0 \tag{37}$$

$$(1+w_n^{\mathrm{II}*})k(\ln v)t^{\mathrm{II}}v^{kw_n^{\mathrm{II}*}+1}L^{\mathrm{II}}+1=0 \tag{38}$$

5.1　负外部性下的最优信息安全投资与潜在损失

分别对式(37)和式(38)应用隐函数的求导法则，可得

$$\frac{\partial w_n^{\mathrm{I}*}}{\partial L^{\mathrm{I}}}=\frac{(w_n^{\mathrm{I}*}+1)vt^{\mathrm{I}}}{2(kw_n^{\mathrm{I}*}+1)-vt^{\mathrm{I}}L^{\mathrm{I}}} \tag{39}$$

$$\frac{\partial w_n^{\mathrm{II}*}}{\partial L^{\mathrm{II}}}=-\frac{(1+w_n^{\mathrm{II}*})}{[1+(1+w_n^{\mathrm{II}*})k(\ln v)]L^{\mathrm{II}}} \tag{40}$$

根据式(34)和式(35)，有

$$\frac{\partial w_n^{\mathrm{I}*}}{\partial L^{\mathrm{I}}}<0 \tag{41}$$

$$\frac{\partial w_n^{\mathrm{II}*}}{\partial L^{\mathrm{II}}}<0 \tag{42}$$

因此，可得到以下定理。

定理 4 在相互博弈的 2 个组织之间呈现负外部性的情况下，面对目标攻击和机会攻击时最优信息安全投资与潜在损失呈负相关关系。

在负外部性条件下，如果组织信息安全投资不足，则会有更大的可能招致攻击，因此，组织有更大的压力进行信息安全投资。由纳什均衡条件式(13)可以看出，相比单一组织的情况，负外部性加大了信息安全投资效益（在同质组织的假定下，由 $|S_1'(w_1)|$ 变为 $|(1+w_1)S_1'(w_1)|$）。而纳什均衡存在的条件式(34)和式(35)说明最优信息安全投资必须受脆弱性等变量的约束。当潜在损失不断升高时，由于信息安全投资已经较大，组织无法继续追加信息安全投资。因此，在负外部性条件下，组织应当着力优化其信息资产，减少潜在损失，因为高潜在损失下企业很难期望使用信息安全投资降低总体损失。

5.2 负外部性下的最优信息安全投资与脆弱性

同理，应用隐函数的求导法则可得

$$\frac{\partial w_n^{\mathrm{I}*}}{\partial v}=\frac{(w_n^{\mathrm{I}*}+1)t^{\mathrm{I}}L^{\mathrm{I}}}{2(kw_n^{\mathrm{I}*}+1)-vt^{\mathrm{I}}L^{\mathrm{I}}} \tag{43}$$

$$\frac{\partial w_n^{\mathrm{II}*}}{\partial v}=-\frac{[1+(1+kw_n^{\mathrm{II}*})k(\ln v)](1+w_n^{\mathrm{II}*})}{[1+(1+w_n^{\mathrm{II}*})k(\ln v)](\ln v)v} \tag{44}$$

根据式(34)和式(35)，有

$$\frac{\partial w_n^{\mathrm{I}*}}{\partial v^{\mathrm{I}}}<0$$

$$[1+(1+w_n^{\mathrm{II}*})k(\ln v)](\ln v)v<0 \tag{45}$$

当 $k<1$ 时，根据式(35)，有 $[1+(1+kw_n^{\mathrm{II}*})k(\ln v)](1+w_n^{\mathrm{II}*})>0$，当 $k>1$ 时，在 v 较小时则可能出现 $[1+(1+kw_n^{\mathrm{II}*})k(\ln v)]\cdot(1+w_n^{\mathrm{II}*})<0$。

因此，可得到以下定理。

定理 5 在相互博弈的 2 个组织之间呈现负外部性的情况下，当面对目标攻击时，最优信息安全投资随脆弱性的提高而减小；当面对机会攻击时，若信息安全投资效率较小，则最优信息安全投资随脆弱性的提高而增大，反之，若信息安全投资效率较大，则最优信息安全投资随脆弱性的提高先减小后增大。

在面对目标攻击时，由于其受高脆弱性的影响相比机会攻击更小，在信息安全投资已经较高并且存在约束的条件下，最优信息安全投资将随脆弱性的提高而减小。在面对机会攻击时，若信息安全投资效率较小，由于高脆弱性带来的严重影响，组织必须随脆弱性的提高而追加信息安全投资。从式(35)可以看出，若信息安全投资效率较大，则信息安全投资面临的约束也更紧，在低脆弱性的情况下，组织将随脆弱性的提高而降低信息安全投资，而在高脆弱性时仍需要不断追加信息安全投资以弥补损失。由此可见，在负外部性条件下组织比较重视对高脆弱性下机会攻击的抵御，并且必须做好对投资效率的衡量。

5.3 负外部性下的最优信息安全投资与投资效率

分别对式(37)和式(38)应用隐函数的求导法则，可得

$$\frac{\partial w_n^{\mathrm{I}*}}{\partial k}=\frac{(2kw_n^{\mathrm{I}*}+2-vt^{\mathrm{I}}L^{\mathrm{I}})s-vt^{\mathrm{I}}L}{(vt^{\mathrm{I}}L^{\mathrm{I}}-2kw_n^{\mathrm{I}*}-2)k} \tag{46}$$

$$\frac{\partial w_n^{\mathrm{II}*}}{\partial k}=-\frac{(1+w_n^{\mathrm{II}*})[1+w_n^{\mathrm{II}*}k(\ln v)]}{[1+(1+w_n^{\mathrm{II}*})k(\ln v)]k} \tag{47}$$

根据式(34)和式(35)，有

$$\frac{\partial w_n^{\mathrm{I}*}}{\partial k}<0 \tag{48}$$

$$\frac{\partial w_n^{\mathrm{II}*}}{\partial k}<0 \tag{49}$$

因此，可得到以下定理。

定理 6 在相互博弈的 2 个组织之间呈现负外部性的情况下，面对目标攻击和机会攻击时最优信息安全投资与投资效率呈负相关关系。

通过式(6)和式(7)可以看出漏洞概率函数对投资效率的导数为负，投资效率的增长本来对漏洞风险有降低的作用，并且高投资效率会带来更严格的投资约束。在负外部性条件下，由于较高的投资水平以及投资约束的存在，伴随投资效率的增长，组织不需再追加信息安全投资，而主要利用较高的投资效率达到一定的安全水平。

总体而言，相较正外部性的情况，组织在负外部性条件下虽然存在更大的激励，但信息安全投资伴随潜在损失、脆弱性和投资效率的增长变得更加谨慎。所以组织对于自己与其他组织关系的判断至关重要。从此再次看出信息安全投资是兼顾“科学”与“艺术”的问题，需要充分的经济学考量，难以

通过纯粹的技术手段解决。

6　社会最优下的最优信息安全投资

之前的内容主要研究的是博弈条件下基于个体理性得出的最优信息安全投资额。在社会最优情况下，全体福利达到最高，此时，个体的支付与博弈条件下往往不同。将社会最优下的最优信息安全投资与博弈条件下的情况做对比，有助于进一步认清外部性对信息安全投资和总体收益的影响特点。

在正外部性条件下，总体收益为

$$E_{sp}(w_1,w_2)=\{tv-S_1(w_1)+[1-aS_1(w_1)]qS_2(w_2)\}L+\{tv-S_2(w_2)+[1-aS_2(w_2)]qS_1(w_1)\}L-w_1-w_2 \tag{50}$$

通过分析其最优解可得

$$S'(w_{sp}^*)=-\frac{1}{[1+aq-2aqS(w_{sp}^*)]L} \tag{51}$$

由式(20)得，在正外部性下的最优信息安全投资额满足 $S'(w_p^*)=-\frac{1}{[1-aqS(w_p^*)]L}$。因此，可得 $w_p^*<w_{sp}^*$。由于在 $w_p^*\neq w_{sp}^*$ 处必有 $E_{sp}(w_p^*)<E_{sp}(w_{sp}^*)$，因此，在正外部性下的社会最优收益大于独立博弈时的总体收益。

同理，在负外部性条件下，总体收益为

$$E_{sn}(w_1,w_2)=[tv-S_1(w_1\mathrm{e}^{w_1-w_2})]L+[tv-S_2(w_2\mathrm{e}^{w_2-w_1})]L-w_1-w_2 \tag{52}$$

通过分析其最优解可得

$$S'(w_{sn}^*)=-\frac{1}{L} \tag{53}$$

即在负外部性条件下，社会最优下信息安全投资的最优解与 Gordon-Loeb 模型一致。由式(36)可知，在负外部性下的最优信息安全投资额满足 $S'(w_n^*)=-\frac{1}{(1+w_n^*)L}$。因此，可得 $w_n^*>w_{sn}^*$。同理，由于 $w_n^*\neq w_{sn}^*$，所以 $E_{sn}(w_n^*)<E_{sn}(w_{sn}^*)$，即在负外部性下的社会最优收益大于独立博弈时的总体收益。

综上，可得以下定理。

定理 7　相比独立博弈的情况，社会最优时的总体收益更大，并且在正外部性下的信息安全投资更大，在负外部性下的信息安全投资更小。

根据分析，正外部性与负外部性分别对信息安全投资有抑制和促进的作用，这种作用在独立博弈的情况下表现更明显，社会最优对这种偏低或偏高的投资额有一定的调节作用。

7　结束语

本文通过分析信息安全投资存在的外部性，基于 Gordon-Loeb 模型建立了组织信息安全投资博弈模型，分别研究了正外部性和负外部性条件下对目标攻击和机会攻击时最优信息安全投资的变化情况。主要结论可以归纳如下。

1) 在正外部性条件下，最优信息安全随潜在损失和脆弱性的变化情况与 Gordon-Loeb 模型存在相似之处，说明正外部性对组织信息安全投资的影响并不深入。组织在进行信息安全投资时，面对潜在损失、脆弱性和投资效率的增大，都至少在这些参数较小时出现信息安全投资的增长期。因此，组织在正外部性下的信息安全投资总体较为积极。

2) 负外部性条件下最优信息安全投资的变化规律与正外部性时反差较大。除了在面对机会攻击并且脆弱性较高时，组织的信息安全投资表现较为消极。因此组织必须善于控制信息安全投资。

3) 面对目标攻击和机会攻击时最优信息安全投资的变化情况与这 2 种攻击的特点相关程度很高，例如，由于高脆弱性下机会攻击更难被抵御，当脆弱性增大时，组织必须在外部性环境下根据攻击类型做出是否追加投资的选择。

4) 社会最优的要求增大了总体收益，其对最优信息安全投资额的影响与外部性所具有的特点有关。

总之，客观条件对组织的信息安全投资提出了较高的要求。组织必须善于分析内外部环境，合理估计各种参数，才能正确地进行投资，否则可能产生适得其反的效果。另外，本文研究也有很多不足，例如，对攻击类型可以有更加细致的划分，攻击者可以被作为博弈参与方，并考虑多阶段的博弈交互，这些可以作为未来研究的改进方向。

参考文献：

[1] ANDERSON R. Why information security is hard: an economic perspective[C]//The Seventeenth Annual Computer Security Applications Conference. 2001: 358-365.

[2] GORDON L A, LOEB M P. The economics of information security investment[J]. ACM Transactions on Information & System Security, 2002, 5(4):438-457.

[3] 陈天平, 张串绒, 郭威武, 等. 效用理论在信息安全投资优化中的应用[J]. 计算机科学, 2009, 36(12):70-72.

CHEN T P, ZHANG C R, GUO W W, et al. Application of utility theory in investment optimizing of information security[J]. Computer Science, 2009, 36(12):70-72.

[4] GORDON L A, LOEB M P, LUCYSHYN W, et al. Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model[J]. Journal of Information Security, 2015, 6(1):24-30.

[5] HUANG C D, HU Q, BEHARA R S. Economics of information security investment in the case of simultaneous attacks[C]//The Fifth Workshop on the Economics of Information Security. 2006.

[6] HUANG C D, HU Q, BEHARA R S. An economic analysis of the optimal information security investment in the case of a risk-averse firm[J]. International Journal of Production Economics, 2008, 114(2): 793-804.

[7] HUANG C D, BEHARA R S, GOO J. Optimal information security investment in a Healthcare Information Exchange: an economic analysis[J]. Decision Support Systems, 2013, 61(1):1-11.

[8] GORDON L A, LOEB M P, LUCYSHYN W. Sharing information on computer systems security: an economic analysis[J]. Journal of Accounting & Public Policy, 2003, 22(6):461-485.

[9] 巩国权, 王军, 强爽. 双寡头垄断市场的信息安全投资模型研究[J]. 中国管理科学, 2007, 15(z1):444-448.
GONG G Q, WANG J, QIANG S. Information security investment model in dual-oligopoly market[J]. Chinese Journal of Management Science, 2007, 15(z1):444-448.

[10] LELARGE M. Coordination in network security games: a monotone comparative statics approach[J]. IEEE Journal on Selected Areas in Communications, 2012, 30(11): 2210-2219.

[11] WU Y, FENG G, WANG N, et al. Game of information security investment: impact of attack types and network vulnerability[J]. Expert Systems with Applications, 2015, 42(15-16):6132-6146.

[12] QIAN X, LIU X, PEI J, et al. A game-theoretic analysis of information security investment for multiple firms in a network[J]. Journal of the Operational Research Society, 2017, 68(10):1-16.

[13] IOANNIDIS C, PYM D, WILLIAMS J. Fixed costs, investment rigidities, and risk aversion in information security: a utility-theoretic approach[M]//Economics of Information Security and Privacy III. 2013: 171-191.

[14] ČAPKO Z, AKSENTIJEVIĆ S, TIJAN E. Economic and financial analysis of investments in information security[C]//The 37th International Convention on Information and Communication Technology, Electronics and Microelectronics. 2014:1550-1556.

[作者简介]

王秦（1990-），男，甘肃天水人，中央财经大博士生，主要研究方向为信息安全的经济学分析。

朱建明（1965-），男，山西太原人，博士，中央财经大学教授、博士生导师，主要研究方向为信息安全和电子商务安全。