Management Science and Engineering 管理科学与工程, 2025, 14(1), 124-136
Published Online January 2025 in Hans. https://www.hanspub.org/journal/mse
https://doi.org/10.12677/mse.2025.141014

Hans汉斯

黑客参与下企业信息安全投资与定价决策研究

耿文艳，吴　勇

东华大学旭日工商管理学院，上海

收稿日期：2024年12月17日；录用日期：2025年1月8日；发布日期：2025年1月20日

摘　要

随着信息网络通信技术的发展，企业面临着越来越多的信息安全挑战。由于市场规模有限，商业环境的日渐复杂，企业之间往往存在一定程度的竞争。随着消费者越来越关注信息安全，企业之间的竞争也从单方面的价格竞争发展到价格和安全的双重竞争，价格和安全共同影响着企业的市场规模。在这样的背景下，本文将策略黑客作为理性参与者，构建了价格和安全双重竞争的企业和策略黑客之间的博弈理论模型，通过逆向归纳法求解得到企业在单独决策和联合决策下的均衡决策。紧接着，本文采用比较静态分析的方法，详细探讨了价格竞争、安全竞争等核心要素对于企业均衡决策和期望收益的影响。此外，通过对比两种模式下的均衡决策，发现企业在单独决策时存在安全努力扭曲问题。因此，本文提出了基于安全努力的合作机制来协调企业的安全努力，从而达到社会最优安全水平。最后，本文分析了上述核心要素对于该机制的影响并验证了该机制的有效性。

关键词

信息安全，竞争企业，策略黑客，机制设计

Research on Firm Information Security Investment and Pricing Decision with Hacker Participation

Wenyan Geng, Yong Wu

Glorious Sun School of Business & Management, Donghua University, Shanghai

Received: Dec. 17th, 2024; accepted: Jan. 8th, 2025; published: Jan. 20th, 2025

Abstract

With the development of information network communication technology, firms are facing more and more information security challenges. Due to the limited size of the market and the increasing

文章引用: 耿文艳, 吴勇. 黑客参与下企业信息安全投资与定价决策研究[J]. 管理科学与工程, 2025, 14(1): 124-136.
DOI: 10.12677/mse.2025.141014

complexity of the business environment, there is often a certain degree of competition between firms. As consumers become more and more concerned about information security, the competition among firms has developed from unilateral price competition to dual competition of price and security, with price and security jointly affecting the market size of firms. In such a background, this paper takes strategic hackers as rational participants, constructs a game theoretical model between firms and strategic hackers with dual competition of price and security, and solves the equilibrium decisions of firms under individual decision and joint decision by backward induction. After that, this paper adopts the method of comparative static analysis to explore in detail the impact of core elements such as price competition and security competition on the equilibrium decision and expected payoff of firms. In addition, by comparing the equilibrium decisions under the two models, we found that there exists the distortion problem of the security effort under the In-house model. To address this problem, we propose the cooperative mechanism based on security efforts to coordinate the security efforts of firms so as to achieve the socially optimal security level. Finally, we analyze the effect of the above core elements on the mechanism and verify the effectiveness of the mechanism.

Keywords

Information Security, Competitive Firm, Strategic Hacker, Mechanism Design

1. 引言

随着数字经济时代的演进，数据成为企业重要的信息资产和战略资源，在助力企业快速发展的同时，也给企业带来了许多的信息安全挑战，愈演愈烈的数据泄露态势，成为企业发展道路上的严重阻碍。《2024年上半年数据泄露风险态势报告》显示[1]，2024年上半年全网监测并分析验证有效的数据泄露事件16,011起，较2023年下半年增长59.58%。数据泄露事件层出不穷，给企业带来了巨额的经济损失。《2024年数据泄露成本报告》指出[2]，70%的受访企业认为数据泄露给他们带来了重大甚至灾难性的损失。

由于信息安全事件的高发性和高危性，近年来，各行各业对信息安全的关注度不断攀升。信息安全在很长一段时间内被认为是一个计算机技术问题，研究者们重点关注的是如何提高安全技术，如更高级的防火墙、完善的入侵检测系统、复杂的加密协议以及访问控制机制等。尽管技术手段在不断更新和完善，但是信息安全事件仍然层出不穷，而且造成的后果越来越严重。这一现象促使研究者们开始反思并逐渐认识到信息安全管理不仅需要提高安全技术，还需要制定经济激励制度，因此，许多研究者将经济因素考虑到信息安全管理领域。Anderson 和 Moore (2006) [3]在《Science》上发表文章总结了信息安全经济学这一新兴学科的发展历程、学科特色以及研究前景，将其定义为：信息安全经济学将各种经济和社会因素考虑在内，运用经济和管理相关理论，解决信息安全参与者的利益冲突，并最终提供合理的信息安全管理策略。

正如传统经济学中探讨的，价格竞争广泛存在于企业之间。然而，随着消费者越来越关注信息安全，企业竞争已经从单方面的价格竞争扩大到价格和安全的双重竞争。消费者在面对行业中的竞争企业时，不仅会比较两家企业的产品价格，还会评估两家企业的安全水平。当一家企业付出更多的安全努力来保护其信息系统免遭安全漏洞时，消费者与该企业进行交易的焦虑就会减弱，从而增强消费者对该企业产品的信心，提高他们的付费意愿。反之，如果竞争对手加强了安全措施，相比之下，该企业会被认为不

那么可靠和安全，最终会导致该企业的消费者流失。

在这样的背景下，本文构建了一个博弈理论模型。在该模型中，两家竞争企业通过决策产品价格和安全努力来进行博弈，并试图回答以下问题：第一，黑客参与下两家竞争企业的均衡价格和安全策略是什么？第二，黑客的变现率和安全损失如何影响企业的安全努力、产品价格和期望收益？第三，企业付出的安全努力是否可以达到社会最优水平，如果不能，是否有合理的激励机制可以协调企业的安全努力？交叉影响和重叠影响如何影响这一机制？第四，黑客参与下，各个博弈主体的均衡决策是什么？核心参数是如何影响博弈主体的均衡决策以及期望收益的？黑客的参与会影响上述研究结论吗？

2. 文献综述

本文的研究领域主要涉及以下两个方面：信息安全经济学、黑客行为和机制设计。

随着信息技术的快速发展，网络安全问题变得越来越严重，数据泄露、黑客攻击等问题时有发生。在首届 WEIS 论坛上，信息安全大师 Bruce Schneier 坦言指出“网络安全不是一个技术能够解决的问题”。这促使研究者们开始反思并逐渐认识到信息安全管理不仅需要提高安全技术，还需要制定经济激励制度，经济学的核心思想是资源稀缺性和资源的优化配置，对于信息安全来说，同样存在着资源稀缺和资源有效利用问题[4]。Gordon 和 Loeb (2002)在他们的开创性研究中，将经济学模型引入到信息安全领域，研究在考虑信息资产脆弱性的情况下，单个企业以最大化自身的期望收益为目标进行的最优安全投资决策，研究发现在给定的潜在损失水平下，由于保护脆弱性中等的信息资产成本较低，因此，企业应将安全投入集中在此类信息资产上[5]。此后很多学者基于 Gordon 和 Loeb 提出的模型进行了深入研究。随着商业环境的日益复杂，信息安全经济学被应用于特定的细分领域，如竞争领域[6]-[9]、供应链领域[10]-[12]及其他领域。Gal-Or 和 Ghose (2005)构建了一个决策模型，研究信息共享组织中两个竞争企业的最优决策问题，并进一步分析了竞争强度和企业规模对最优决策的影响[8]。Cezar 等(2017)通过建立分析模型，研究风险相互依赖性和竞争外部性对企业安全决策的影响[6]。Wu 等(2022)构建了博弈理论模型，研究在考虑技术相似性的情况下，竞争行业中企业的最优安全决策问题[13]。此外，熊强等(2012)依据供应链上企业关系的非对等性，运用 Stackerlberg 模型讨论了供应链中的核心企业和伙伴企业在信息安全方面的决策博弈，得出企业信息资产价值、网络脆弱性、共享成本、信息安全互补性等因素对决策结果的影响机制[12]。Luo 和 Choi (2022)构建了一个博弈理论框架，分析供应链中企业间的互动，并研究政府对企业安全决策的影响[14]。赵柳榕等(2020)考虑声誉、共享效率、信息安全风险等因素，基于演化博弈分析了供应链企业间的信息安全共享行为，并探讨了共享成本和安全风险的变化对双方决策的影响[15]。董坤祥等(2021)研究了强制性约束下企业信息安全投资和网络保险的最优决策问题，并分析了可观测和不可观测企业损失时的最优投资策略[16]。

作为信息安全领域的重要参与者和利益相关方，现有研究中，有关其攻击模式的研究比较广泛，通常分为定向攻击和随机攻击。Gao 等(2015)讨论了在面对两种攻击类型的情况下，竞争企业的安全投资策略，研究发现黑客采用定向攻击比采用随机攻击能够获得更高的期望收益[17]。潘崇霞等(2019)构建了期望效用模型，同时考虑了随机攻击与定向攻击两种攻击类型、信息共享、决策者风险偏好、两企业之间的投资博弈等因素，分别对随机攻击与定向攻击情形下的两个风险厌恶型企业的信息安全投资策略进行了研究[18]。然而，现有研究中有关黑客行为的研究较少。Cavusoglu 等(2014)运用博弈论模型分析了企业该如何运用 IDS 进行技术配置，研究发现企业只要根据外部黑客入侵调整 IDS 技术配置就能够带来收益[19]。Gao 等(2014)运用微分博弈论，研究了两家竞争企业在有目标攻击下的安全投资和信息共享的动态策略，即两家企业都可以通过定价的内生决定来影响其信息资产的价值[20]。Hausken (2017)从黑客之间的信息共享的角度出发，探究企业如何防范日益复杂的黑客，研究发现企业对两个黑客的防御增加了黑客的单位成本，降低了黑客的信息共享效率和联合共享的利用，也降低了双方黑客的声誉收益[21]。Wu

等(2022)根据黑客的攻击目的，将黑客分为追求收益和追求名誉的黑客，并建立了博弈理论分析模型，研究企业与这两种类型的黑客之间的战略互动，研究发现，不同的攻击目的会产生不同的黑客行为[13]。

为了解决多个企业在互动过程中由于利益不一致产生的安全努力的扭曲问题，需要设计合理的激励机制来协调企业的投资动机。Wu 等(2015)建立了一个博弈理论分析模型并设计了责任机制和安全信息共享机制，以协调企业面临不同攻击类型时的安全投资[22]。Qian 等(2018)通过构建纳什均衡、部分集中决策和完全集中决策三种模型，研究了企业在不同模型下的信息共享和安全投资策略，并提出了协调企业投资策略的两种补偿机制[10]。Wu 等(2021)利用基于努力的机制和基于责任的机制来解决在考虑信息资产性质和技术相似性的情况下企业之间的搭便车问题[23]。刘艺浩等(2023)基于外部性不对称视角研究了安全标准约束下的信息安全部分外包，研究发现，当企业采取核心外包策略时，在较低的强制性安全标准约束下，企业需要设立赔偿机制从而得到最低期望成本[24]。Gao 等(2024)通过构建可替代企业与策略黑客之间的博弈理论模型，研究了可替代企业的安全投资和信息共享决策，研究发现，尽管广泛使用的补偿机制可以促使企业在安全损失保持较低水平时增加投资，但由于过度投资，补偿机制会增加企业的预期成本[25]。

3. 问题描述与模型建立

3.1. 问题描述

本章节中，我们研究了两个竞争企业和策略黑客之间的博弈，两家企业记为企业 i 和企业 j。我们假设两家企业提供差异化的产品(或服务)并且消费者依据产品(或服务)的两个维度来做出购买决策：产品价格和安全质量。

我们构建了一个两阶段博弈。第一阶段：企业同时决策信息安全质量，即企业所付出的安全努力，记为 s_i 和 s_j，同时，策略黑客决策针对这两个竞争企业施加的攻击努力，记为 z_i 和 z_j。第二阶段：企业同时做出定价决策，记为 p_i 和 p_j。遵循先前的研究[6] [8]，我们假设企业做出安全努力决策先于定价决策，原因有二：其一，我们的研究聚焦于安全相关的行业，包括智能汽车、电子商务、消费金融、快递物流以及其他消费者相对更加关注信息安全的行业，因此，企业在做出定价决策时需要考虑到自身的信息安全状况。其二，与定价决策相比，企业的安全努力决策更具战略性和长期性，而定价决策则相对灵活多变。

我们引入企业 i 的产品需求函数，记为 D_i。请注意，为了便于后文描述，我们将聚焦的企业描述为企业 i，其竞争对手描述为企业 j。D_i 取决于产品价格 p 和安全努力 s，于是我们有 $D_i\left(p,s\right)=\alpha-p_i+\omega p_j+g_i\left(s_i,s_j\right)$。

我们假设每种产品的需求是关于自身价格 p_i 和竞争对手价格 p_j 的线性函数。为了聚焦研究重点并简化模型符号，我们将企业自身价格 p_i 对产品需求的影响系数归一化为 1。此外，由于市场中存在价格竞争，竞争对手的价格 p_j 对企业 i 的产品需求也有积极的影响。具体而言，模型中参数 $\alpha>0$ 表示潜在的市场需求，而参数 ω 的大小反映了企业之间价格竞争的程度。我们进一步假设相较于企业自身的定价决策，价格竞争对企业产品需求的影响是次要的，因此，我们有 $0<\omega<1$。

$g_i\left(s_i,s_j\right)$ 反映了产品安全质量对需求的影响。下面我们继续阐述 $g_i\left(s_i,s_j\right)$ 是如何依赖于企业自身的安全努力 s_i 的和竞争对手的安全努力 s_j 的。毫无疑问，$g_i\left(s_i,s_j\right)$ 会随着 s_i 的增加而增加。企业增加安全努力，如强化防火墙技术、完善安全策略等，那么信息系统被破坏的可能性就会降低，从而打消消费者与企业进行交易的顾虑，增加企业的市场需求。我们引入参数 $\varphi>0$ 来表示企业自身的安全努力 s_i 对产品需求的影响。影响越大，意味着企业自身的安全努力越有利于其产品需求。因此，我们用 φs_i 表示企业自身的安全努力 s_i 对产品需求的影响。然而，随着竞争对手的安全努力 s_j 的增加，一方面，由于企业 j 提供了更高的安全水平，消费者可能更倾向于与企业 j 进行交易，因此，由于市场中存在安全竞争，企业 j 的安全努力 s_j 对企业 i 的产品需求会产生消极影响。我们引入参数 ε 来反映企业之间安全竞争的程度。此外，我们假设相较于企

业自身的安全努力，安全竞争对企业产品需求的影响是次要的，因此，我们有$0<\varepsilon<\varphi$。我们用εs_j表示竞争对手的安全努力s_j对产品需求的消极影响。因此，我们有$g_i\left(s_i,s_j\right)=\varphi s_i-\varepsilon s_j$。

因此，我们将企业i的产品需求函数总结如下：

$$D_i=\alpha-p_i+\omega p_j+\varphi s_i-\varepsilon s_j, i\neq j$$

现实中，企业所采取的信息系统安全保护措施一直在不断发展和演化。从一开始的防火墙和防病毒软件等基础的设施技术，到后来的身份验证和访问管理，再到如今的区块链技术，企业在安全配置和管理方面的投入也在不断增加。因此，我们用$C\left(s_i\right)$表示企业i的安全努力成本。遵循先前的研究[26]-[28]，我们假设企业i的安全努力成本$C\left(s_i\right)$具有两种特征：一是$C\left(s_i\right)$随着安全努力s_i的增加而增加，二是$C\left(s_i\right)$是关于s_i的凹函数，即$\frac{\partial C\left(s_i\right)}{\partial s_i}\geq 0$，$\frac{\partial^2 C\left(s_i\right)}{\partial s_i^2}>0$。在本文中，我们给定$C\left(s_i\right)$为$cs_i^2$，其中$c>0$表示安全努力成本系数。

当企业i被黑客入侵时，它将遭受一定的安全损失，包括有形损失(如信息资产和劳动力)和无形损失(如品牌声誉和市场价值)。因此，我们用L_i表示黑客攻击给企业i造成的安全损失。请注意，安全损失的程度还可以反映企业的规模，因为一旦黑客成功发起攻击，大型企业会遭受更大程度的安全损失[29]。同时，当黑客成功入侵企业i时，黑客会将攻击所得在黑客市场上进行交易，从而获得收入。我们引入参数$a>0$来表示攻击所得在黑客市场上的变现率[17]。为了简化符号，我们将黑客的攻击概率表示如下：

$$P_i=z_i\left(1-s_i\right)$$

表 1 总结了本章节涉及的主要符号及含义。

Table 1. Key symbols and meanings
表 1. 关键符号及含义

符号	含义
s_i	企业i的安全努力
p_i	企业i的产品价格
z_i	黑客对企业i的攻击努力
D_i	企业i的产品的市场需求
P_i	企业i遭受黑客攻击的概率
L_i	黑客攻击给企业i造成的安全损失
a	安全损失的变现率
ρ	攻击努力的成本系数
α	潜在的市场规模
φ	自身安全努力对需求的影响
ω	价格竞争程度
ε	安全竞争程度
π_i	企业i的期望收益
c	安全努力的成本系数

3.2. 模型建立

首先，我们讨论了这两家竞争企业以最大化自身的期望收益为目标，独立进行价格和安全努力决策的情况，此时，企业i的期望收益包括销售收入、安全努力成本和黑客攻击造成的安全损失。因此，我们

可以将企业 i 的期望收益表示如下：

$$\pi_i = p_i D_i - c s_i^2 - P_i L_i$$

其中，$D_i = \alpha - p_i + \omega p_j + \varphi s_i - \varepsilon s_j, i \neq j$。

我们假设这两家竞争企业具有对称的特征。黑客以最大化自身的期望收益为目标做出攻击努力决策。黑客的期望收益包括将攻击所得在黑市上变现的收入以及发起安全攻击的成本。因此，我们可以将黑客的期望收益表示如下：

$$\pi_H = P_i\left(aL_i\right) + P_j\left(aL_j\right) - \rho z_i^2 - \rho z_j^2$$

我们假设企业和黑客同时决策。这意味着每个博弈方的决策都是对另一博弈方做出的外生给定策略的最优反应。接下来，我们用逆向归纳法来求解。在第二阶段，对于给定的安全努力 s_i 和攻击努力 z_i，我们可以刻画出企业的均衡产品价格，这也被称作价格的反应函数。我们在定理 3-1 中刻画了均衡产品价格随着安全努力的变化情况。在第一阶段，我们可以进一步得到企业的均衡安全努力和黑客的均衡攻击努力。我们在定理 3-2 中总结了企业在单独决策时各个博弈主体的均衡决策。

定理 3-1：(1) 企业的产品价格总是随着自身安全努力的增加而增加，即 $\frac{\partial p_i}{\partial s_i} > 0$；(2) 当安全竞争程度相对较低时，企业的产品价格随着竞争对手安全努力的增加而增加；当安全竞争程度相对较高时，企业的产品价格随着竞争对手安全努力的增加而减少，即 $\begin{cases} \frac{\partial p_i}{\partial s_j} > 0, & 0 \le \varepsilon < \frac{\varphi\omega}{2} \\ \frac{\partial p_i}{\partial s_j} < 0, & \frac{\varphi\omega}{2} < \varepsilon < \varphi \end{cases}$。

证明：定理 3-1 的证明包含在定理 3-2 的证明中。

根据定理 3-1(1)，我们发现企业的产品价格总是随着自身安全努力的增加而增加。企业加强安全努力，其市场需求会随之增加，因此，企业会选择提高产品价格($\frac{\partial p_i}{\partial s_i} > 0$)。定理 3-1(2)指出，企业的产品价格随着竞争对手安全努力的变化情况取决于企业之间的安全竞争程度。当安全竞争程度相对较低时($0 \le \varepsilon < \frac{\varphi\omega}{2}$)，企业的产品价格随着竞争对手安全努力的增加而增加，原因如下：由于企业之间存在安全竞争，当竞争对手增加安全努力时，企业自身也会增加安全努力以获取竞争优势，根据定理 3-1(1)，此时企业会提高产品价格；当安全竞争程度相对较高时($\frac{\varphi\omega}{2} < \varepsilon < \varphi$)，企业的产品价格随着竞争对手安全努力的增加而减少，这是由于竞争对手安全努力的增加意味着企业 i 面临消费者损失的风险(εs_j)增加，此时企业会选择降低价格以吸引更多需求($\frac{\partial p_i}{\partial s_j} < 0$)。

定理 3-2：单独决策时，企业 i 的均衡产品价格为

$$p^H = \frac{\left(a\left(-\alpha-\varphi+\varepsilon\right)L^2 - 4\alpha c\rho\right)\left(\omega-2\right)\left(\omega+2\right)}{\left(-a\left(\omega+2\right)\left(\omega-2\right)^2\right)L^2 - 4\rho\left(\left(\left(\omega+2\right)\left(\omega-2\right)^2\right)c - \left(-\alpha+\varepsilon\right)\left(\varepsilon\omega-2\varphi\right)\right)}$$，均衡安全努力为

$$s^H = \frac{\left(-a\left(\omega+2\right)\left(\omega-2\right)^2\right)L^2 + 4\alpha\rho\left(\varepsilon\omega-2\varphi\right)}{\left(-a\left(\omega+2\right)\left(\omega-2\right)^2\right)L^2 - 4\rho\left(\left(\left(\omega+2\right)\left(\omega-2\right)^2\right)c - \left(-\alpha+\varepsilon\right)\left(\varepsilon\omega-2\varphi\right)\right)}$$，黑客的均衡攻击努力为

$$z^H = \frac{2a\left(\left(-\left(\omega+2\right)\left(\omega-2\right)^2\right)c + \left(\varepsilon\omega-2\varphi\right)\left(-\alpha-\varphi+\varepsilon\right)\right)L}{\left(-a\left(\omega+2\right)\left(\omega-2\right)^2\right)L^2 - 4\rho\left(\left(\left(\omega+2\right)\left(\omega-2\right)^2\right)c - \left(-\alpha+\varepsilon\right)\left(\varepsilon\omega-2\varphi\right)\right)}$$。

证明：两家竞争企业的期望收益函数关于价格的一阶导为：$\begin{cases}\dfrac{\partial \pi_i}{\partial p_i}=-\varepsilon s_j+\omega p_j+\varphi s_i+\alpha-2p_i\\ \dfrac{\partial \pi_i}{\partial p_j}=-\varepsilon s_j+\omega p_j+\varphi s_i+\alpha-2p_i\end{cases}$。联立求解，我们可以得到给定安全努力 s_i 时企业的均衡产品价格，即价格的反应函数：

$\begin{cases}p_i=\dfrac{(\varepsilon\omega-2\varphi)s_j+(2\varepsilon-\omega\varphi)s_i-\alpha\omega-2\alpha}{\omega^2-4}\\ p_j=\dfrac{(\varepsilon\omega-2\varphi)s_j+(2\varepsilon-\omega\varphi)s_i-\alpha\omega-2\alpha}{\omega^2-4}\end{cases}$。价格反应函数的一阶导为：$\begin{cases}\dfrac{\partial p_i}{\partial s_i}=\dfrac{\partial p_j}{\partial s_j}=\dfrac{\varepsilon\omega-2\varphi}{\omega^2-4}\\ \dfrac{\partial p_i}{\partial s_j}=\dfrac{\partial p_j}{\partial s_i}=\dfrac{2\varepsilon-\varphi\omega}{\omega^2-4}\end{cases}$，因此，我们有 $\dfrac{\partial p_i}{\partial s_i}>0$；$\begin{cases}\dfrac{\partial p_i}{\partial s_j}>0,\ 0\le\varepsilon<\dfrac{\varphi\omega}{2}\\ \dfrac{\partial p_i}{\partial s_j}<0,\ \dfrac{\varphi\omega}{2}<\varepsilon<\varphi\end{cases}$。

定理 3-1 得证。

将均衡价格代入期望收益函数中，联立企业的期望收益函数关于安全努力的一阶导和黑客的期望收益函数关于攻击努力的一阶导，最终我们可以得单独决策时企业以及黑客的均衡决策。

定理 3-2 得证。

为了衡量企业所付出的安全努力的程度，我们将这两家竞争企业作为一个整体，进一步讨论企业以最大化整体的期望收益为目标，联合进行价格和安全努力决策的情况。在联合决策的情况下，我们可以将企业 i 的期望收益表示如下：

$$\pi=p_iD_i-cs_i^2-P_iL_i+p_jD_j-cs_j^2-P_jL_j$$

其中，$D_i=D_j=\alpha-p_i+\omega p_j+\varphi s_i-\varepsilon s_j, i\neq j$。

同样，我们在定理 3-3 中展示了联合决策下企业以及黑客的均衡决策。

定理 3-3：在联合决策下，企业 i 的均衡产品价格为 $p^B=\dfrac{-aL^2(-\alpha-\varphi+\omega)-4\alpha c\rho}{2aL^2(\omega-1)+2\rho\left(4c(\omega-1)+(-\varphi+\varepsilon)^2\right)}$，均衡安全努力为 $s^B=\dfrac{\alpha\rho(-\varphi+\varepsilon)+aL^2(\omega-1)}{aL^2(\omega-1)+\rho\left(4c(\omega-1)+(-\varphi+\varepsilon)^2\right)}$，黑客的均衡攻击努力为 $z^B=\dfrac{aL\left(4c(\omega-1)+(-\alpha-\varphi+\varepsilon)(-\varphi+\varepsilon)\right)}{8\rho c(\omega-1)+2\rho(-\alpha+\varepsilon)^2+2aL^2(\omega-1)}$。

证明：定理 3-3 的证明与定理 3-2 类似，因此，这里我们不再赘述。

通过比较单独决策和联合决策下的企业的均衡决策，我们可以得到以下命题。

命题 3-1：当安全竞争相对较高时，单独决策时企业的安全努力高于联合决策。

证明：根据定理 3-1 和定理 3-2，我们有 $\begin{cases}s^H-s^B<0,\ 0\le\varepsilon<\varepsilon_1\\ s^H-s^B>0,\ \varepsilon_1<\varepsilon<\varphi\end{cases}$，即 $\begin{cases}s^H<s^B,\ 0\le\varepsilon<\varepsilon_1\\ s^H>s^B,\ \varepsilon_1<\varepsilon<\varphi\end{cases}$，其中，$\varepsilon_1=\dfrac{\omega\alpha\left(\omega^2-2\omega+4\right)}{\omega^3+2\omega^2-8\omega+8}$。

命题 3-1 得证。

命题 3-1 表明，在黑客参与的情况下，与联合决策相比，当安全竞争程度不同时，企业倾向于投资

不足或投资过度。直觉上，我们认为企业在联合决策下的安全努力总是高于单独决策[30]。在一定的安全竞争程度下($0 \le \varepsilon < \varepsilon_1$)，正如预期的那样，我们确实发现联合决策下的均衡安全努力高于单独决策。回顾定理 3-1(2)，当安全竞争程度不太高时，企业的均衡产品价格随着竞争对手安全努力的增加而增加，企业会减小安全努力。然而，当安全竞争程度相对较高时($\varepsilon_1 < \varepsilon < \varphi$)，我们发现了与直觉相反的结论：与单独决策相比，联合决策下的安全努力反而更低。这是因为过高的安全竞争程度意味着一旦竞争对手增加安全努力，那么企业面临的消费者流失风险(εs_j)增加，因此，企业会为了获得竞争优势而过度投资。而联合决策的内部化效应有效地抑制了竞争企业的过度投资，因此呈现出更低但更理性的安全努力。

4. 比较静态分析

首先我们讨论了黑客变现率 a 对企业均衡安全努力 s^H、均衡产品价格 p^H 和黑客均衡攻击努力 z^H 的影响。

命题 4-1：企业的均衡安全努力 s^H、均衡产品价格 p^H 和黑客的均衡攻击努力 z^H 总是随着黑客变现率的增加而增加，即 $\frac{\partial s^H}{\partial a} > 0$，$\frac{\partial p^H}{\partial a} > 0$，$\frac{\partial z^H}{\partial a} > 0$。

证明：企业的均衡安全努力 s^H、均衡产品价格 p^H 和黑客的均衡攻击努力 z^H 分别对 a 求导，我们有

$$\frac{\partial s^H}{\partial a} = \frac{-\rho\left(\left(-(\omega+2)(\omega-2)^2\right)c + (-\alpha-\varphi+\varepsilon)(\varepsilon\omega-2\varphi)\right)(\omega+2)(\omega-2)^2 L^2}{4M^2} > 0,$$

$$\frac{\partial p^H}{\partial a} = \frac{-\rho\left(\left(-(\omega+2)(\omega-2)^2\right)c + (-\alpha-\varphi+\varepsilon)(\varepsilon\omega-2\varphi)\right)(\omega+2)(\omega-2)(-\varphi+\varepsilon)L^2}{4M^2} > 0,$$

$$\frac{\partial z^H}{\partial a} = \frac{\rho\left(\left(-(\omega+2)(\omega-2)^2\right)c + (-\alpha-\varphi+\varepsilon)(\varepsilon\omega-2\varphi)\right)L\left(\left(-(\omega+2)(\omega-2)^2\right)c + (-\varphi+\varepsilon)(\varepsilon\omega-2\varphi)\right)}{2M^2} > 0,$$ 其中，$M = \left(-\rho(\omega+2)(\omega-2)^2\right)c + \left(\frac{-a(\omega+2)(\omega-2)^2}{4}\right)L^2 + \rho(-\varphi+\varepsilon)(\varepsilon\omega-2\varphi)$。

命题 4-1 得证。

命题 4-1 表明，企业的均衡安全努力 s^H、均衡产品价格 p^H 和黑客的均衡攻击努力 z^H 总是随着黑客变现率的增加而增加。对于黑客来说，加强攻击努力一方面会带来更高的收入，这是积极影响；另一方面也会导致更高的攻击成本，这是消极影响。随着黑客变现率的增加，黑客将攻击所得在黑客市场上变现的收入增加，由此产生的积极影响占主导地位。因此，黑客有动机增加攻击努力($\frac{\partial z^H}{\partial a} > 0$)。面对黑客攻击，企业不得不增加安全努力来保护其信息系统($\frac{\partial s^H}{\partial a} > 0$)，同时，企业会提高产品价格来支撑安全方面的投入($\frac{\partial p^H}{\partial a} > 0$)。

接下来，我们分析了攻击损失 L 对企业均衡安全努力 s^H、均衡产品价格 p^H 和黑客均衡攻击努力 z^H 的影响。

命题 4-2：企业的均衡安全努力 s^H、均衡产品价格 p^H 和黑客的均衡攻击努力 z^H 总是随着攻击损失的增加而增加，即 $\frac{\partial s^H}{\partial L} > 0$，$\frac{\partial p^H}{\partial L} > 0$，$\frac{\partial z^H}{\partial L} > 0$。

证明：企业的均衡安全努力 s^H、均衡产品价格 p^H 和黑客的均衡攻击努力 z^H 分别对 L 求导，我们有

$$\frac{\partial s^H}{\partial L}=\frac{-a\rho\left(\left(-(\omega+2)(\omega-2)^2\right)c+(-\alpha-\varphi+\varepsilon)(\varepsilon\omega-2\varphi)\right)(\omega+2)(\omega-2)^2 L}{2M^2}>0,$$

$$\frac{\partial p^H}{\partial L}=\frac{-a\rho\left(\left(-(\omega+2)(\omega-2)^2\right)c+(-\alpha-\varphi+\varepsilon)(\varepsilon\omega-2\varphi)\right)(\omega+2)(\omega-2)(-\varphi+\varepsilon)L}{2M^2}>0,$$

$$\frac{\partial z^H}{\partial L}=\frac{a\left(\left(-(\omega+2)(\omega-2)^2\right)c+(-\alpha-\varphi+\varepsilon)(\varepsilon\omega-2\varphi)\right)\left(\left(-\rho(\omega+2)(\omega-2)^2\right)c+\left(\frac{a(\omega+2)(\omega-2)^2}{4}\right)L^2+\rho(-\varphi+\varepsilon)(\varepsilon\omega-2\varphi)\right)}{2M^2}>0$$

其中，$M=\left(-\rho(\omega+2)(\omega-2)^2\right)c+\left(\frac{-a(\omega+2)(\omega-2)^2}{4}\right)L^2+\rho(-\varphi+\varepsilon)(\varepsilon\omega-2\varphi)$。

命题 4-2 得证。

如前所述，L 不仅可以衡量企业规模，还反映了黑客攻击给企业 i 造成的安全损失。正如预期的那样，命题 4-2 表明，随着安全损失的增加，企业将不遗余力地加强安全努力以免遭受黑客入侵给企业带来灾难性的损失($\frac{\partial s^H}{\partial L}>0$)，同时，企业会提高产品价格来维持收益稳定($\frac{\partial p^H}{\partial L}>0$)。对于黑客来说，一方面由于企业加强安全努力，安全水平得到了提高，这意味着黑客需要付出更高的攻击成本，这是消极影响；另一方面，黑客一旦成功入侵，将获得可观的收入，这是积极影响。随着安全损失的增加，黑客通过发起攻击获得的收入不断增加，积极影响占主导地位，因此，黑客有动机加强攻击努力($\frac{\partial z^H}{\partial L}>0$)。

接下来，我们详细探讨了上述关键因素分别对企业和黑客期望收益的影响。

命题 4-3：黑客的期望收益总是随着变现率和安全损失的增加而增加，即 $\frac{\partial \pi_H}{\partial a}>0$，$\frac{\partial \pi_H}{\partial L}>0$。

证明：黑客的期望收益函数分别对 a，L 求导，我们有

$$\frac{\partial \pi_H}{\partial a}=\frac{aL^2\rho^2\left(\left(-(\omega+2)(\omega-2)^2\right)c+(\varepsilon\omega-2\varphi)(-\alpha-\varphi+\varepsilon)\right)^2\left(\left(-(\omega+2)(\omega-2)^2\right)c+(\varepsilon\omega-2\varphi)(-\varphi+\varepsilon)\right)}{R^3}>0,$$

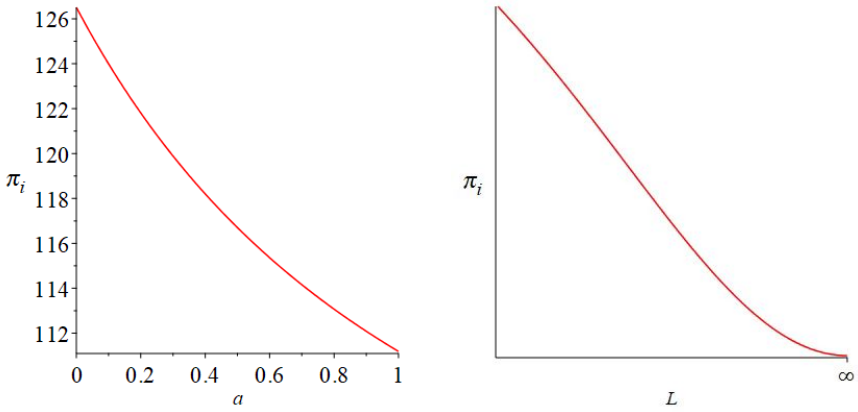
$$\frac{\partial \pi_H}{\partial L}=\frac{a^2L\rho\left(\left(-(\omega+2)(\omega-2)^2\right)c+(\varepsilon\omega-2\varphi)(-\alpha-\varphi+\varepsilon)\right)^2\left(\left(\left(-4(\omega+2)(\omega-2)^2\right)c-4(\alpha-\varepsilon)(\varepsilon\omega-2\varphi)\right)\rho+aL^2(\omega+2)(\omega-2)^2\right)}{R^3}>0$$

命题 4-3 得证。

命题 4-3 表明，黑客的期望收益总是随着变现率和安全损失的增加而增加。根据黑客的期望收益函数可知，对于黑客来说，一方面变现率和安全损失的增加给黑客带来了更高的收入，这是积极影响；另一方面结合命题 4-1 和命题 4-2，黑客的均衡攻击努力随着变现率和安全损失的增加而增加，因此，变现率和安全损失的增加同时还给黑客带来了更高的成本，这是消极影响。随着变现率和安全损失的增加，黑客主动加强攻击努力，由此带来的积极影响更加突出，因此，黑客的期望收益会增加。

接下来，我们使用以下参数对企业的期望收益函数 π_i 随着变现率 a 和安全损失 L 的变化情况进行数值分析：$\varepsilon=5$，$\varphi=10$，$\omega=0.2$，$\alpha=20$，$c=100$，$\rho=70$ (改变这些参数取值仍然可以得到类似的结果)。

图 1 表明，企业的期望收益总是随着变现率和安全损失的增加而减少。回顾命题 4-1、命题 4-2，企业的均衡安全努力 s^H、均衡产品价格 p^H 和黑客的均衡攻击努力 z^H 随着变现率和安全损失的增加而增加，因此，对于企业来说，价格增加带来的收入增加效应和安全努力增加带来的成本上涨效应对企业的期望收益构成相反的影响。变现率和安全损失的增加诱使黑客加强攻击努力，因此，企业不得不增加安全努力来保护其信息系统，由此带来的成本上涨效应更加突出，因此，企业的期望收益会减少。



(a) π_i 随着 a 的变化情况　　(b) π_i 随着 L 的变化情况

Figure 1. The variation of π_i with respect to changes in a and L

图 1. π_i 随着 a 和 L 的变化情况

5. 机制设计

首先，我们将联合决策下企业的安全努力定义为社会最优安全努力。命题 3-1 表明，在黑客参与的情况下，当两家竞争企业独立进行安全决策时，会产生安全努力的扭曲问题。为了解决这一问题，本节提出了基于企业安全努力的合作机制来协调企业的投资动机。合作机制允许付出安全努力的一方从对方企业获得一定数量的奖励，反之亦然。也就是说，如果企业 i 付出了安全努力 s_i，那么企业 i 在付出安全成本 cs_i^2 的同时会获得企业 j 的投资回报 $\xi_j s_i$。我们用 $\xi_i\left(\xi_j\right)$ 来表示在黑客参与的情况下，企业付出安全努力的奖励率。在期望收益函数中引入奖励后，我们将期望收益函数重写为：

$$\pi_i = p_i D_i - cs_i^2 - P_i L_i + \xi_j s_i - \xi_i s_j$$

其中，$D_i = \alpha - p_i + \omega p_j + \varphi s_i - \varepsilon s_j, i \neq j$。

为了能够准确观察到对方企业的安全努力，企业通常需要引入第三方机构的监测。我们假设安全努力可以被监测，也就意味着可以被第三方验证。互联网促进了跨组织对信息的实时访问[31]。在实践中，IT 支持的服务和跨区域人员主要负责监测企业的安全努力。RosettaNet 和 GS1 是全球标准组织，它们为企业之间的通信开发通用平台，以实现跨组织(甚至在全球范围内)的协作和交易自动化。这些标准和其他 IT 支持的服务有助于实时数据传输和自动化通信[32]。此外，合作各方通常会组织跨区域的人员定期举行会议、电话会议、演讲等[33]。因此，实践表明各方的安全努力可以被监测和验证。

显然，监测对方企业的安全努力会给企业带来相关的成本。我们将监测成本记为 Φ。在某些情况下，如果安全努力增加，那么相应的监测成本也会更高。换句话说，如果企业付出的安全努力较低，那么就更容易被监测到。因此，我们分析了监测成本 Φ 随着安全努力的增加而增加(即 $\frac{\partial \Phi}{\partial s_i} \geq 0$)的情况。研究发现，将 Φ 视为常数还是变量并不会改变本文的主要见解。因此，本文将 Φ 视为常数。在期望收益函数中引入监测成本后，我们将期望收益函数重写为：

$$\pi_i = p_i D_i - cs_i^2 - P_i L_i + \xi_j s_i - \xi_i s_j - \Phi$$

其中，$D_i = \alpha - p_i + \omega p_j + \varphi s_i - \varepsilon s_j, i \neq j$。

通过求解一阶导，令合作机制下的安全努力与社会最优安全努力相等，我们发现 $\xi_i = \xi_j = \xi$。定理 5-1 总结了我们的研究发现。

定理 5-1：合作机制下，当奖励率为 $\xi=\xi^*$ 时，企业将达到社会最优安全努力。

证明：合作机制下，企业的期望收益函数关于价格的一阶导为 $\begin{cases}\dfrac{\partial\pi_i}{\partial p_i}=-\varepsilon s_j+\omega p_j+\varphi s_i+\alpha-2p_i\\ \dfrac{\partial\pi_i}{\partial p_j}=-\varepsilon s_i+\omega p_i+\varphi s_j+\alpha-2p_j\end{cases}$。对于给定的安全努力 s_i，企业的均衡产品价格为 $\begin{cases}p_i=\dfrac{(\varepsilon\omega-2\varphi)s_i+(2\varepsilon-\omega\varphi)s_j-\alpha b-2\alpha}{b^2-4}\\ p_j=\dfrac{(\varepsilon\omega-2\varphi)s_i+(2\varepsilon-\omega\varphi)s_j-\alpha b-2\alpha}{b^2-4}\end{cases}$。将 p_i 和 p_j 代入 π_i，通过最大化均衡产品价格下企业的期望收益函数，我们得到均衡安全努力 $s_i=s_j=s^*$。根据定理 3-3 可知，社会最优安全努力为 $s^B=\dfrac{\alpha\rho(-\varphi+\varepsilon)+aL^2(\omega-1)}{aL^2(\omega-1)+\rho\left(4c(\omega-1)+(-\varphi+\varepsilon)^2\right)}$。令 $s^*=s^B$，于是我们有 $\theta_i=\theta_j=\theta=\theta^*$。此外，我们发现 $\begin{cases}\xi^*>0,\ 0\le\varepsilon<\varepsilon_1\\ \xi^*<0,\ \varepsilon_1\le\varepsilon<\varphi\end{cases}$，其中 $\varepsilon_1=\dfrac{\omega\varphi(\omega^2-2\omega+4)}{\omega^3+2\omega^2-8\omega+8}$。

定理 5-1 得证。

命题 4-4：当重叠程度相对较低时，奖励率为正，当重叠程度相对较高时，奖励率为负，即 $\begin{cases}\xi^*>0,\ 0\le\varepsilon<\varepsilon_1\\ \xi^*<0,\ \varepsilon_1\le\varepsilon<\varphi\end{cases}$。

证明：命题 4-4 的证明包含在定理 5-1 的证明中。

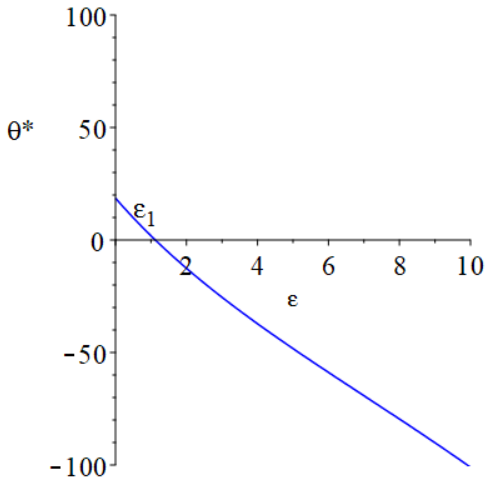


Figure 2. The variation of θ^* with respect to changes in θ^*

图 2. 奖励率 θ^* 随着 θ^* 的变化情况

定理 5-1 表明，在黑客参与的情况下，合作机制可以引导企业达到社会最优安全努力，从而解决安全努力的扭曲问题。此外，命题 4-4 表明，当安全竞争程度相对较低时，奖励率为正，反之，奖励率为负。回顾命题 3-1，当安全竞争程度相对较低时，企业在联合决策下的安全努力低于单独决策，此时，为了达到社会最优安全努力，企业会获得投资回报，从而增加企业的投资动机。反之，当安全竞争程度相对较高时，企业在单独决策下的安全努力高于联合决策，此时，为了达到社会最优安全努力，企业会获

得投资惩罚，从而减少企业的投资动机。

接下来，我们通过数值仿真进一步验证上述结论的稳健性。图 2 展示了奖励率 ξ^* 随着安全竞争程度 ε 的变化情况，其中 $\varphi=10$，$\omega=0.2$，$\alpha=20$，$c=100$，$\rho=70$，$a=0.1$ (改变这些参数取值仍然可以得到类似的结果)。

6. 结论与展望

随着信息网络通信技术的发展，企业面临着越来越多的信息安全挑战。由于市场规模有限，商业环境的日渐复杂，企业之间往往存在一定程度的竞争。随着消费者对信息安全的关注度不断攀升，企业之间的竞争已经由单方面的价格竞争发展为价格和安全的双重竞争。因此，本文引入策略黑客，构建了价格安全双重竞争的企业和黑客之间的博弈理论模型，研究了各个博弈主体以最大化自身的期望收益为目标的均衡决策，并进一步探讨了黑客变现率、安全损失等核心要素对于企业均衡决策和期望收益的影响。此外，通过将企业在单独决策和联合决策时的均衡决策进行对比，我们发现黑客参与下，企业在单独决策时存在安全努力的扭曲问题。因此，本文提出了基于安全努力的合作机制来协调企业的安全努力，从而达到社会最优安全水平。此外，本文获得了一些管理启示，可以帮助企业在实践中做出科学合理的安全决策。

本文研究了在黑客参与下价格和安全双重竞争的企业和黑客之间的战略互动。尽管上述研究结论确实值得关注，但本文仍存在一些局限性。例如，我们假设每家企业的产品类型都是单一的，但实践中企业通常会根据产品价值来实施安全措施。为了获得更多的见解，未来的研究可以进一步探讨产品价值与安全努力之间的关系，从而获得更多有趣的见解。

参考文献

[1] 澎湃新闻·澎湃号·湃客. 2024 年上半年数据泄露风险态势报告[EB/OL]. https://www.thepaper.cn/newsDetail_forward_27963751, 2024-07-05.

[2] IBM 发布《2024 年数据泄露成本报告》: 企业数据泄露成本创新高, AI 和自动化成为“数据保卫战”突破口[R]. 2024.

[3] Anderson, R. and Moore, T. (2006) The Economics of Information Security. *Science*, **314**, 610-613. https://doi.org/10.1126/science.1130992

[4] 刘雪灵, 刘祎果, 裴兰. 信息安全经济学的国际前沿研究概况[J]. 中国信息安全, 2013(10): 68-71.

[5] Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, **5**, 438-457. https://doi.org/10.1145/581271.581274

[6] Cezar, A., Cavusoglu, H. and Raghunathan, S. (2017) Sourcing Information Security Operations: The Role of Risk Interdependency and Competitive Externality in Outsourcing Decisions. *Production and Operations Management*, **26**, 860-879. https://doi.org/10.1111/poms.12681

[7] Gao, X. and Zhong, W. (2016) A Differential Game Approach to Security Investment and Information Sharing in a Competitive Environment. *IIE Transactions*, **48**, 511-526. https://doi.org/10.1080/0740817x.2015.1125044

[8] Gal-Or, E. and Ghose, A. (2005) The Economic Incentives for Sharing Security Information. *Information Systems Research*, **16**, 186-208. https://doi.org/10.1287/isre.1050.0053

[9] Kolfal, B., Patterson, R.A. and Yeo, M.L. (2013) Market Impact on IT Security Spending. *Decision Sciences*, **44**, 517-556. https://doi.org/10.1111/deci.12023

[10] Qian, X., Liu, X., Pei, J. and Pardalos, P.M. (2017) A New Game of Information Sharing and Security Investment between Two Allied Firms. *International Journal of Production Research*, **56**, 4069-4086. https://doi.org/10.1080/00207543.2017.1400704

[11] Wu, Y., Feng, G. and Fung, R.Y.K. (2018) Comparison of Information Security Decisions under Different Security and Business Environments. *Journal of the Operational Research Society*, **69**, 747-761. https://doi.org/10.1057/s41274-017-0263-y

[12] 熊强, 仲伟俊, 梅姝娥. 基于 Stackelberg 博弈的供应链企业间信息安全决策分析[J]. 情报杂志, 2012, 31(2): 178-182, 167.

[13] Wu, Y., Xiao, H., Dai, T. and Cheng, D. (2021) A Game-Theoretical Model of Firm Security Reactions Responding to

a Strategic Hacker in a Competitive Industry. *Journal of the Operational Research Society*, **73**, 716-740. https://doi.org/10.1080/01605682.2020.1854631

[14] Luo, S. and Choi, T. (2022) E-Commerce Supply Chains with Considerations of Cyber-Security: Should Governments Play a Role? *Production and Operations Management*, **31**, 2107-2126. https://doi.org/10.1111/poms.13666

[15] 赵柳榕, 杨广文, 邹文轩, 刘健楠. 考虑声誉的供应链企业间信息安全共享演化博弈研究[J]. 数学的实践与认识, 2020, 50(16): 285-291.

[16] 董坤祥, 谢宗晓, 甄杰. 强制性约束下企业信息安全投资与网络保险的最优决策分析[J]. 中国管理科学, 2021, 29(6): 70-81.

[17] Gao, X. and Zhong, W. (2015) Information Security Investment for Competitive Firms with Hacker Behavior and Security Requirements. *Annals of Operations Research*, **235**, 277-300. https://doi.org/10.1007/s10479-015-1925-2

[18] 潘崇霞, 仲伟俊, 梅姝娥. 不同攻击类型下风险厌恶型企业信息安全投资策略[J]. 系统工程学报, 2019, 34(4): 497-510.

[19] Cavusoglu, H., Raghunathan, S. and Yue, W.T. (2008) Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, **25**, 281-304. https://doi.org/10.2753/mis0742-1222250211

[20] Gao, X., Zhong, W. and Mei, S. (2014) A Game-Theoretic Analysis of Information Sharing and Security Investment for Complementary Firms. *Journal of the Operational Research Society*, **65**, 1682-1691. https://doi.org/10.1057/jors.2013.133

[21] Hausken, K. (2017) Information Sharing among Cyber Hackers in Successive Attacks. *International Game Theory Review*, **19**, Article ID: 1750010. https://doi.org/10.1142/s0219198917500104

[22] Wu, Y., Feng, G., Wang, N. and Liang, H. (2015) Game of Information Security Investment: Impact of Attack Types and Network Vulnerability. *Expert Systems with Applications*, **42**, 6132-6146. https://doi.org/10.1016/j.eswa.2015.03.033

[23] Wu, Y., Wang, L., Cheng, D., *et al.* (2021) Information Security Decisions of Firms Considering Security Risk Interdependency. *Expert Systems with Applications*, **178**, Article ID: 114990. https://doi.org/10.1016/j.eswa.2021.114990

[24] 刘艺浩, 吴勇. 安全标准约束下的信息安全部分外包研究——基于外部性不对称视角[J]. 管理科学与工程, 2023, 12(1): 1-18.

[25] Gao, X., Zhang, Y., Zhong, B., Wang, X. and Wang, Y. (2024) A Duopolistic Analysis of CEO Competitive Aggressiveness with R&D Investment. *Production and Operations Management*, **33**, 1083-1098. https://doi.org/10.1177/10591478241238971

[26] Kim, B.C., Chen, P. and Mukhopadhyay, T. (2011) The Effect of Liability and Patch Release on Software Security: The Monopoly Case. *Production and Operations Management*, **20**, 603-617. https://doi.org/10.1111/j.1937-5956.2010.01189.x

[27] Nagurney, A. and Shukla, S. (2017) Multifirm Models of Cybersecurity Investment Competition vs. Cooperation and Network Vulnerability. *European Journal of Operational Research*, **260**, 588-600. https://doi.org/10.1016/j.ejor.2016.12.034

[28] Yang, M., Jacob, V.S. and Raghunathan, S. (2021) Cloud Service Model's Role in Provider and User Security Investment Incentives. *Production and Operations Management*, **30**, 419-437. https://doi.org/10.1111/poms.13274

[29] Ponemon (2019) Cost of a Data Breach Report 2019. Poneomon Institute. https://doi.org/10.1016/S1361-3723(19)30081-8

[30] Qian, X., Liu, X., Pei, J., Pardalos, P.M. and Liu, L. (2017) A Game-Theoretic Analysis of Information Security Investment for Multiple Firms in a Network. *Journal of the Operational Research Society*, **68**, 1290-1305. https://doi.org/10.1057/s41274-016-0134-y

[31] Swaminathan, J.M. and Tayur, S.R. (2003) Models for Supply Chains in E-Business. *Management Science*, **49**, 1387-1406. https://doi.org/10.1287/mnsc.49.10.1387.17309

[32] Erhun, F. and Keskinocak, P. (2011) Collaborative Supply Chain Management. *Planning Production and Inventories in the Extended Enterprise*: *A State of the Art Handbook*, **1**, 233-268. https://doi.org/10.1007/978-1-4419-6485-4_11

[33] Choudhury, V. and Sabherwal, R. (2003) Portfolios of Control in Outsourced Software Development Projects. *Information Systems Research*, **14**, 291-314. https://doi.org/10.1287/isre.14.3.291.16563