Management Science and Engineering 管理科学与工程, 2024, 13(1), 292-306
Published Online January 2024 in Hans. https://www.hanspub.org/journal/mse
https://doi.org/10.12677/mse.2024.131029

Hans汉斯

考虑安全标准的互补企业信息安全决策研究

王　楠，吴　勇

东华大学旭日工商管理学院，上海

收稿日期：2023年11月28日；录用日期：2024年1月22日；发布日期：2024年1月31日

摘　要

随着全球合作化的深入，企业间信息不再彼此独立而是呈现出一种互补的信息资产结构。为了应对越来越频繁的信息安全事件，很多企业选择将安全外包给专业的安全管理服务提供商(MSSP)。此外，政府也逐渐开始重视企业的信息安全管理，会通过安全标准和安全补贴等措施来试图提高企业的安全水平。本文基于企业的互补信息特征，研究了在考虑安全标准时，互补企业在不同安全条件下的最优信息安全决策，也为实际的安全决策提供一定的管理启示。本文发现无论是内部管理还是安全外包，随着安全补贴的增加，企业和MSSP都会提高安全质量。但是过于严格的强制安全标准会让企业选择将安全外包给MSSP来规避责任，即使企业知道MSSP不会实际提供和强制安全标准一样的安全质量。此外，本文发现当企业选择自我管理时，严格的强制安全标准会扭曲企业的均衡行为，造成不必要的社会福利损害。

关键词

信息安全外包，互补企业，安全标准，外包风险

Research on Information Security Decision of Complementary Firms Considering Security Standard

Nan Wang, Yong Wu

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

Received: Nov. 28th, 2023; accepted: Jan. 22nd, 2024; published: Jan. 31st, 2024

Abstract

With the deepening of global cooperation, information among firms is no longer independent, but presents complementation each other. To solve more and more frequent information security in-

文章引用: 王楠, 吴勇. 考虑安全标准的互补企业信息安全决策研究[J]. 管理科学与工程, 2024, 13(1): 292-306.
DOI: 10.12677/mse.2024.131029

cidents, many firms choose to outsource security to managed security service providers (MSSP). In addition, the government gradually begins to pay attention to the information security management, and try to improve the firm's security level through security standard and security subsidy. Based on the complementary information characteristics of firms, this paper studies the firm's optimal information security decisions under different security conditions when considering security standard, and also provides some management implications for practical security decisions. This study finds that both firms and MSSPs improve the security quality as security subsidy increases, whether managed in-house or outsourced. But overly strict mandatory security standard may induce firms to choose to outsource security to MSSP to avoid security liability, even when firms know that MSSPs do not actually provide the same security quality as the mandatory security standard. In addition, we find that when firms choose to manage in-house, strict mandatory security standard can distort firms' equilibrium behavior and cause unnecessary social welfare damage.

Keywords

Security Outsourcing, Complementary Firm, Scurity Standard, Outsourcing Risks

1. 引言

随着各行各业的数字化转型的持续深入，各种新兴信息技术虽然给社会生产生活活动带来了便利，但是也带来了越来越频繁的信息安全事件。信息安全已成为很多企业面临的重大挑战。在信息安全威胁下，企业面临着两种选择：内部安全管理或将安全管理外包给安全管理服务提供商(Managed Security Service Provider，以下简称为 MSSP)。因此信息技术的日益复杂，将信息安全外包给 MSSP 也成为企业的一种有效策略。MSSP 提供安全服务范围包括外包安全管理和监控企业的安全系统和设置。据 Statista 报告显示，到 2026 年，MSSP 市场预计价值约 640 亿美元[1]。

虽然 MSSP 在安全管理上具有很多优势，例如成本效益、更合规和责任转移，但也面临着诸多挑战，尤其是安全外部性和信息泄露风险。对于安全外部性，由于 MSSP 的成本效益，MSSP 服务于多个客户公司在实践中是常见的[2]。此时，MSSP 具有显著的安全外部性，即 MSSP 对一家企业的安全投资可能会影响其他企业的安全，但是正面和负面的安全外部性会对 MSSP 产生不同的影响，对于信息泄露风险，导致信息泄露问题的根本原因是客户公司信息向 MSSP 的迁移[3]。因此，当客户公司将信息安全外包时，MSSP 可能有意或无意地向外部透露客户的敏感信息造成额外的损失。

为了提高运营效率，在实践中，企业之间的信息通常以互补的形式存在[4]。当企业信息具有互补性时，黑客需要先攻破一家企业，然后再成功攻破另一家企业，从而获得更多价值，单个企业的信息对黑客来说价值不大。一个飞机制造商的例子可以很好地说明信息资产的互补性：商业飞机将新飞机主要部件的设计外包给供应商公司。如果黑客想要获得关于整个新飞机设计的商业情报，黑客必须从飞机公司和供应商公司获得完整的设计信息[5]。

此外，除了企业和 MSSP 这些安全管理主体，近几年政府和行业监管机构也在逐渐注重信息安全管理，陆续出台了多个安全标准对数据安全进行监管。信息安全有关的强制性制度的颁布和实施对企业的信息安全部署产生了重要深刻的影响。2022 年英国发布的新版《国家网络战略》中，英国政府将投资 26

亿英镑用于网络和传统信息技术行业，并且为国家网络安全计划增加 1.14 亿英镑以增加网络韧性来应对网络威胁[6]。这些数据安全有关规定要求企业在日常数据管理中达到相关安全标准，例如定期审察日志，采用明确的报告标准等。政府等监管机构通过网络安全审查、安全标准制定等措施，促使企业在满足特定安全水平要求下，提高应对风险能力，以保障网络空间安全。

本文以互补企业作为研究基础，考虑有安全标准和政府安全补贴时，两个互补企业内部自我管理和外包给 MSSP 两种情景下的信息安全决策，试图回答不同安全标准的最优信息安全决策的问题，也给企业信息安全管理给与一定的管理启示。

2. 文献综述

本文的研究领域主要涉及以下几个方面：信息资产互补，信息安全外包和安全标准。

在对信息资产是互补关系的企业研究中，研究者主要研究互补的信息资产性质是如何影响企业的信息安全投资决策的。Liu 等(2011)研究了信息共享程度对互补企业信息安全决策的影响，发现企业不需要外部因素的诱导就有分享安全知识的动机[5]。Gao 等(2014)研究了信息互补的两个企业的信息分享和安全投资，并且考虑了社会规划者对企业安全投资的激励，结果发现第三方的协调并不是有用的[7]。Wu 等(2017)将原来研究的完全互补替代扩展为部分互补替代，研究了互补或者替代程度对于外包时 MSSP 安全投资的影响[8]。Li (2020)分析了互补型企业在非合作和合作情况下的信息安全投资，发现新企业能够给现有企业带来新知识，并对现有企业产生正向影响[9]。Qian 等(2021)研究了在考虑信息安全保险情况下，具有互补信息资产的两家企业之间的信息安全投资博弈，结果发现联合决策可以使企业更多的预期利润[10]。

在学术上首次对信息安全外包进行系统阐述的是 Rowe (2007)，文章中界定了信息安全外包的内涵，评价了外包的优势和劣势以及梳理了外包合同的设计[11]。关于信息安全外包一个重要研究方向就是研究外包的影响因素，和本文研究相关的安全外部性和信息泄露风险也是被广泛研究的因素。Anderson 等(2008)和 lee 等(2013)发现积极的安全外部性可以允许 MSSP 使用从其他客户公司获得的信息来阻止已识别的攻击，但是负安全外部性会带来战略黑客转移[12] [13]。Cezar 等(2017)发现外包的外部性可分为正外部性和负外部性，企业的外包决策是由外部性的类型(正面或者负面)和外部性程度决定的[14]。赵柳榕等(2019)利用博弈论构建了竞争企业的信息安全决策模型，分析系统内在脆弱性、安全系统相似性、收益转移和外部性因素对安全决策的影响[15]。Feng 等(2020)在外包情景下考虑到信息泄露风险，并且发现信息泄露风险会影响企业的安全外包决策[16]。Wu 等(2021)研究了动态合作环境下系统相互依赖性对于安全外包投资的影响[17]。以往的信息安全外包文献大多假设客户企业间的信息资产是独立的，但是本文还考虑了互补信息资产性质对于安全外包的影响。

目前在安全标准领域中的研究并不多，研究大多集中在安全标准对企业和 MSSP 的安全决策的影响。Hui 等(2012)分析了安全外包时，系统相互依赖风险和强制安全需求对影响 MSSP 和企业均衡结果的影响，并且发现在无法辨别 MSSP 安全努力的情况下，MSSP 可能会提供给安全标准更低的安全努力[18]。Gao 和 Xing(2015)发现外部给定的安全标准需求和企业间的竞争程度会影响企业的信息安全投资决策，当竞争激烈时，企业希望有更严格的安全标准，当竞争程度温和时，企业都希望选择宽松的安全标准[7]。Lee 等(2016)发现更高的安全标准并不一定导致更高的企业安全，并且考虑了当某些安全投资没有得到验证时，安全标准对于企业安全水平的影响[19]。Hui 等(2019)发现当存在安全标准时，为了给客户企业提供更好的服务，MSSP 会更加努力地进行安全投入来满足制定的安全标准[20]。Gao 等(2022)研究表明，严格的强制性标准并不总是对每个企业都有利，即使企业的信息系统可以得到更好的安全保护[21]。以上研究都发现安全标准可以在一定程度上提高企业的安全水平，但是过高标准并不总是有利于企业，本文在此基

础上开展进一步的研究。

基于以上的文献综述，研究发现目前对于互补企业的信息安全决策，特别是在信息安全外包领域的研究较少。因此，本文结合安全标准和互补的信息资产性质对企业的信息安全决策进行深入研究，可以有效补充相关领域的研究，进一步丰富信息安全管理理论。

3. 问题描述

在进行问题描述前，本文中所出现的关键符号被总结在表 1。

Table 1. Main notations
表 1. 关键符号及含义

符号	参数说明
θ	企业间的互补程度，$\theta \in [0,1]$
q_i	企业 i 的安全质量，$q_i \in [0,1]$
c	企业的成本系数，$c > 0$
a	黑客的攻击概率，$a \in (0,1)$
φ	MSSP 的成本效益，$\varphi \in (0,1]$
L	企业被攻击造成的安全损失
v	企业没有遭受安全攻击时的信息资产
ε	外包时发生信息泄露风险的概率，$\varepsilon \in [0,1]$
e	信息泄露和黑客攻击带来的安全损失的比例
t_i	MSSP i 提供外包服务时收取的费用
d_i	发生安全事件时，MSSP 给企业 i 的赔偿费用
s	政府对安全成本的补贴系数，$s \in [0,1]$

本章考虑两个互补企业在有安全标准和安全补贴时，选择内部自我管理或者将安全外包给 MSSP 的信息安全外包策略问题。研究建模为一个单次博弈的契约问题，其中 MSSP 提供契约，企业接受或拒绝契约。两个互补企业选择不同的安全策略会出现两个情景：两个企业都选择内部自我管理或者两个企业都选择将安全外包给 MSSP。我们用一个一般线性模型 p_i 表示企业 i 的安全系统被攻击并没有成功防御的概率，即 $p_i = a(1-q_i)$。其中 a 表示黑客的攻击概率，q_i 表示为了保护企业 i 的信息资产所提供的安全质量。当两个互补企业都选择外包给 MSSP 时，MSSP 端会出现显著的安全外部性，此时企业 i 被击破概率表现为 $p_i = a(1-q_i - bq_j)$，$b > 0 (b < 0)$ 表示正(负)安全外部性并且 $|b| < 1$。表 2 列表了内部管理和外包情境下企业安全被击破的概率。

Table 2. Breach probability under the two scenarios
表 2. 两种情景下的击破概率

情景	企业内部管理	企业安全外包
击破概率	$a(1-q_i)$	$a(1-q_i - bq_j)$

由于互补企业的信息资产性质，企业 i 和企业 j 之间的信息资产互补程度为 θ，在发生信息安全击破行为后企业 i 遭受到的潜在损失为 L，但是由于企业间的互补信息资产，企业 i 的实际损失与企业间的互

补程度有关。如果两个企业都没有被黑客攻击成功，企业 i 的损失为 0；如果企业 i 被攻击而另一个企业 j 没有被攻击，企业 i 所遭受到的安全损失为 $(1-\theta)L$；如果两个企业都被黑客攻击，黑客获得企业的全部信息，企业 i 遭受到的安全损失为 L。值得注意的是，当企业选择外包给 MSSP，由于信息泄露风险，可能还是遭受信息泄露导致的损失，表达为 $\varepsilon e(1-\theta)L$。

此外，信息安全补贴是政府部门常用的激励措施，目的是为了鼓励安全管理者投入足够的安全措施[22]。当企业选择在内部自我管理时，企业的安全成本为 $\frac{1}{2}(1-s)cq_i^2$，当企业选择将安全外包给 MSSP 时，MSSP 的安全成本为 $\frac{1}{2}(1-s)\varphi cq_i^2$。其中 s 是政府对安全管理者的安全补贴系数，s 的取值范围在 0 到 1 之间，s 越接近于 1 说明政府对安全管理者的补贴越大。$\varphi \in (0,1]$ 代表 MSSP 的成本效益，φ 越接近于 1，MSSP 的安全成本越接近于企业的安全成本[17]。

在实际的信息安全外包领域中，双边退款合同(Bilateral Refund Contract，以下简称为 BRC)被广泛地接受和应用，MSSP 通常会提前列出合同内容，然后由客户企业决定是否购买其服务[18] [19] [20]。在这个模型中，假设如果企业 i 选择外包安全服务给 MSSP，后者 MSSP 将会提供 BRC 给企业 i。此时企业 i 需要支付服务费用 t_i 给 MSSP，但是一旦企业的安全被击破并且遭受信息安全损失，MSSP 需要支付赔偿费用 d_i 给企业。基于以上的假设，接下来我们考虑有安全补贴和安全标准时，企业在不同安全条件下的最优安全决策。

3.1. 基准模型

首先，我们讨论没有安全标准时，两个互补企业选择内部自我管理时的情景。此时两个企业会同时决定自己的最优安全质量，企业 i 被攻击的概率为 $p_i = a(1-q_i)$。企业 i 的预期收益为企业 i 的资产减去被安全击破造成的损失和企业实施安全管理所需要的安全成本，被表示如下：

$$\pi_i^F = v_i - p_i(1-p_j)(1-\theta)L - p_i p_j L - \frac{1}{2}(1-s)cq_i^2 \tag{1}$$

为了简化模型，我们假设两个企业 i 和 j 是同质企业，通过求解一阶收益最大化条件，可以得到企业均衡安全质量 q_I^* 和企业预期收益 π_I^*。其中 π_I^* 是内部企业的保留效用。当企业选择外包时获得的预期收益不低于 π_I^* 时，企业才会愿意将安全外包给 MSSP，否则企业宁愿选择内部管理。

接下来，我们讨论两个互补企业选择外包给 MSSP 时的情景，此时 MSSP 会表示出安全外部性，企业 i 被攻击的概率为 $p_i = a(1-q_i-bq_j)$。在企业接受 BRC 时，企业 i 和 MSSP 的预期收益分别如下所示：

$$\pi_i^F = v_i - t_i - p_i(1-p_j)(1-\theta)L - p_i p_j L - \varepsilon e(1-\theta)L + p_i d_i \tag{2}$$

$$\pi_i^M = t_i - p_i d_i - \frac{1}{2}\varphi(1-s)cq_i^2 \tag{3}$$

因此，MSSP 的优化问题可以如下表示：

$$\max_{t_i,d_i} \ \pi_i^M \tag{4}$$

$$\text{s.t. } q_{II}^* \in \arg\max \ \pi_i^M \tag{5}$$

$$\pi_i^F \geq \pi_I^* \tag{6}$$

q_{II}^* 代表 MSSP 子博弈完美均衡下的安全质量，公式(5)是 MSSP 的激励相容(IC)，MSSP 会保证自己得到最大的预期收益。公式(6)是企业的个人理性约束(IR)，确保企业将其安全外包给 MSSP 时获得不低于内部企业保留效用时的收益。因此，互补企业两种情景下的均衡结果如引理 1 所示。

引理 1：存在政府安全补贴系数 s 时：

(a) 当企业选择自我管理时，企业的最优安全质量为 $q_I^* = \frac{aL(2a\theta-\theta+1)}{2a^2L\theta+(1-s)c}$，企业的预期收益为 $\pi_I^* = \frac{aL\left(aL(1-\theta)^2-2(1-s)(1-\theta+a\theta)\right)}{4La^2\theta+2(1-s)c}$；

(b) 当两个企业选择外包给 MSSP 时，MSSP 的安全质量为 $q_{II}^* = \frac{a(b+1)L(2a\theta-\theta+1)}{2a^2(b+1)^2L\theta+(1-s)\varphi c}$，赔偿费用为 $d_{II}^* = \frac{\varphi cL(2a\theta-\theta+1)}{2a^2(b+1)^2L\theta+(1-s)\varphi c}$。

证明：当企业选择内部管理时，企业预期收益求一阶导得：$\frac{\partial \pi_i^F}{\partial q_i} = -a(1-q_i)\left(1-a(1-q_j)\right)(1-\theta)L-a^2(1-q_i)(1-q_j)L-\frac{1}{2}(1-s)cq_i^2$，由于两个企业在假设中是同质的，联立求解可得企业的最优安全质量：$q_I^* = \frac{aL(2a\theta-\theta+1)}{2a^2L\theta+(1-s)c}$。将 q_I^* 代入企业的收益函数，可得内部管理企业的预期收益：$\pi_I^{F*} = \frac{a^2(1-\theta)^2L^2+2aL\left(2a\theta v+(1-s)\left(c(1-\theta+a\theta)\right)\right)+2(1-s)cv}{4a^2\theta L+2c(1-s)}$。

当企业选择将安全外包给 MSSP 时，利用逆向归纳法求解 BRC 中第一阶段 MSSP 的最优安全质量为：$\begin{cases} abd_i-\varphi(1-s)cq_j+ad_j=0 \\ abd_j-\varphi(1-s)cq_i+ad_i=0 \end{cases}$。把 λ 和 u 作为 IC 和 IR 的拉格朗日系数，MSSP 优化问题的拉格朗日函数可以表示为：

$$\begin{aligned} M = {} & t_i-p_id_i-\frac{1}{2}\varphi(1-s)cq_i^2+t_j-p_jd_j-\frac{1}{2}\varphi(1-s)cq_j^2 \\ & +\lambda_1\left(abd_j-\varphi(1-s)cq_i+ad_i\right)+\lambda_2\left(abd_i-\varphi(1-s)cq_j+ad_j\right) \\ & +u_1\left(v_i-t_i-p_i(1-p_j)(1-\theta)L-p_ip_jL-\varepsilon e(1-\theta)L+p_id_i-\pi_I^{F*}\right) \\ & +u_2\left(v_j-t_j-p_j(1-p_i)(1-\theta)L-p_ip_jL-\varepsilon e(1-\theta)L+p_jd_j-\pi_I^{F*}\right) \end{aligned}$$

。该拉格朗日函数的一阶条件表示如下：$\frac{\partial M}{\partial t_i}=1-\lambda_1=0$，$\frac{\partial M}{\partial t_j}=1-\lambda_2=0$；

$\frac{\partial M}{\partial d_i} = -a\left(-bq_j-q_i+1\right)+\lambda_1a+\lambda_2ab+u_1a\left(-bq_j-q_i+1\right)=0$；

$\frac{\partial M}{\partial d_j} = -a\left(-bq_i-q_j+1\right)+\lambda_2a+\lambda_1ab+u_2a\left(-bq_i-q_j+1\right)=0$；$\frac{\partial M}{\partial \lambda_2} = abd_i-\varphi(1-s)cq_j+ad_j=0$；

$\frac{\partial M}{\partial \lambda_1} = abd_j-\varphi(1-s)cq_i+ad_i=0$；$\frac{\partial M}{\partial u_1} = v_i-t_i-p_i(1-p_j)(1-\theta)L-p_ip_jL-\varepsilon e(1-\theta)L+p_id_i-\pi_I^{F*}=0$；

$\frac{\partial M}{\partial u_2} = v_j-t_j-p_j(1-p_i)(1-\theta)L-p_ip_jL-\varepsilon e(1-\theta)L+p_jd_j-\pi_I^{F*}=0$。通过求解一阶的方程组我们可以得到 $\lambda_1=0$，$\lambda_2=0$，$u_1=1$，$u_2=1$，带入可得简化后的拉格朗日函数：

$M = -\frac{1}{2}\varphi(1-s)c\left(q_i^2+q_j^2\right)-p_i(1-p_j)(1-\theta)L-p_j(1-p_i)(1-\theta)L-2p_ip_jL-2\varepsilon e(1-\theta)L-2\pi_I^{F*}$。过对函数第一阶段进行求解，可以得到外包下的最优安全质量 $q_{II}^* = \frac{a(b+1)L(2a\theta-\theta+1)}{2a^2(b+1)^2L\theta+(1-s)\varphi c}$。此外，最优目标函

数 M 对安全质量 q_i 的二阶导数为 $\frac{\partial^2 M}{\partial q_i^2} = -2\theta La^2 - \varphi(1-s)c < 0$，因此 M 是一个严格的凹函数，并且在 q_{II}^* 时有最大值。将 q_{II}^* 代入 $d_i = \frac{\varphi(1-s)c}{a} q_i$，我们可以得到外包情景下的 MSSP 的最优赔偿费用为 $d_{II}^* = \frac{\varphi cL(2a\theta - \theta + 1)}{2a^2(b+1)^2 L\theta + (1-s)\varphi c}$。将 q_{II}^* 和 d_{II}^* 代入 t_i，可以得到外包情景下的 MSSP 的最优服务费用

$$t_{II}^* = \frac{1}{\left(2a^2(1+\theta)^2\theta L + c\varphi(1-s)\right)^2}\Big(\left(a^4L^3(b+1)^4(4\varepsilon e+1)\right)\theta^3 - c^2\varphi^2(1-s)^2(\varepsilon eL - v) + \left(a^2(b+1)^2(2\varepsilon eL + L - 2v) - 2c\varphi(a+2\varepsilon e)(1-s)\right)\theta^2 + \theta\left(c^2\varphi^2(1-s)^2(a^2+\varepsilon e)L + a^4(b+1)^4L^3 - (1-s)a^2(b+1)^2(2aL + 4\varepsilon e + c\varphi v)\right)\Big) - \pi_I^{F*}$$

。由此，MSSP 的预期收益为 $\pi_{II}^* = \frac{1}{4a^2(b+1)^2\theta L + 2c\varphi(1-s)}\Big(a^2(b+1)^2L^2\left(\theta^2(4\varepsilon e+1)+1\right) - 2Lc\varphi(a+\varepsilon e)(1-s) + 2\left(c\varphi L(1-s)(a+\varepsilon e-a^2) - a^2(b+1)^2L^2(2e\varepsilon+1)\right)\Big) - \pi_I^*$。为了确保安全质量 $q_{II}^* \in (0,1)$，可以得到约束条件：$L < \frac{\varphi(1-s)c}{(b+1)a(1-\theta+2ab\theta)}$，该约束确保企业被击破后不会受到过高的损失，否则企业将始终采用最高级别的安全保护措施。

我们将只考虑政府安全补贴时的安全情景作为模型的基准情况，接下来研究存在安全标准时，企业和 MSSP 的不同信息安全决策。

3.2. 安全标准下的信息安全决策

在本节，我们讨论企业在存在安全标准 q_0 时的信息安全策略。安全标准是指通过第三方监管机构认证并且实施强制性安全需求的设置，在实践中，企业满足这些安全需求并不容易，相比之下，如果客户将其保护外包给专业的 MSSP，也同样可以履行监管建构要求其完成的安全义务[23]。事实上，在信息安全外包领域中，由于信息不对称，大部分研究都假设 MSSP 的安全努力是被无法验证的[18] [19]。为了验证安全标准 q_0 的影响，我们需要考虑两种情景下的信息安全决策：

1) 当 $q_0 \le q_I^* = \frac{aL(2a\theta - \theta + 1)}{2a^2L\theta + (1-s)c}$，此时安全标准比企业自我管理时的安全质量还要低，对安全决策的影响是无关紧要的。

2) 当 $q_0 > q_I^* = \frac{aL(2a\theta - \theta + 1)}{2a^2L\theta + (1-s)c}$，如果企业选择自我管理，它必须施加 q_0 的安全质量，但是外包给 MSSP 时，MSSP 的安全质量并不能被验证。

首先，我们讨论安全补贴且安全标准宽松时的情景，此时，企业选择自我管理或者选择外包给 MSSP 时，均衡结果如引理 2 所示：

引理 2：当安全标准宽松，$q_0 \le \frac{aL(2a\theta - \theta + 1)}{2a^2L\theta + (1-s)c}$ 时，企业自我管理或选择外包给 MSSP 时，企业和 MSSP 的均衡结果不变。

证明：证明过程与引理 1 类似，故在这里省略。

接下来，我们讨论有安全补贴且安全标准严格时的情景。当两个企业都选择自我管理时，内包企业的安全质量必须达到安全标准的 q_0，因此此时企业的预期收益表示为：

$$\pi_i^F = v_i - p_i\left(1-p_j\right)(1-\theta)L - p_i p_j L - \frac{1}{2}(1-s)cq_i^2 \tag{7}$$

$$\text{s.t. } q \geq q_0 \tag{8}$$

此时可以求得企业的安全质量为 $\widetilde{q_I^*}$，企业的预期收益为 $\widetilde{\pi_I^*}$。这里将 $\widetilde{\pi_I^*}$ 作为严格安全标准情况下企业新的保留效用，通过逆向归纳法求解可以求出在严格安全标准下，MSSP 的均衡安全质量 $\widetilde{q_{II}^*}$、服务费用 $\widetilde{d_{II}^*}$、赔偿费用 $\widetilde{t_{II}^*}$ 和预期收益 $\widetilde{\pi_{II}^*}$。因此，企业和 MSSP 的均衡结果如引理 3 所示：

引理 3：当安全标准严格，$q_0 > \dfrac{aL(2a\theta-\theta+1)}{2a^2L\theta+(1-s)c}$ 时，

(a) 当企业选择自我管理时，企业的最优安全质量为 $\widetilde{q_I^*} = q_0$，企业的预期收益为 $\widetilde{\pi_I^*} = a(1-q_0)\left(1-\theta-a\theta(1-q_0)\right)L - \dfrac{1}{2}(1-s)cq_0^2$

(b) 当两个企业选择外包给 MSSP 时，MSSP 的最优安全质量和赔偿费用保持不变，分别为 $\widetilde{q_{II}^*} = \dfrac{a(b+1)L(2a\theta-\theta+1)}{2a^2(b+1)^2L\theta+(1-s)\varphi c}$、$\widetilde{d_{II}^*} = \dfrac{\varphi cL(2a\theta-\theta+1)}{2a^2(b+1)^2L\theta+\varphi c}$。

证明：当 $q_0 > \dfrac{aL(2a\theta-\theta+1)}{2a^2L\theta+(1-s)c}$ 时，安全标准大于企业的最优安全质量，那么内部管理企业必须施加 q_0 的安全质量。将企业的安全质量 q_0 代入收益函数，可得企业的预期收益为 $\widetilde{\pi_I^*} = a(1-q_0)\left(1-\theta-a\theta(1-q_0)\right)L - \dfrac{1}{2}(1-s)cq_0^2$。当企业选择外包给 MSSP 时，证明过程与引理 1 类似，故省略。类似地，MSSP 的最优服务费用为：

$$\widetilde{t_{II}^*} = \frac{1}{\left(2a^2(1+\theta)^2\theta L + c\varphi(1-s)\right)^2}\Big(\left(a^4L^3(b+1)^4(4\varepsilon e+1)\right)\theta^3 - c^2\varphi^2(1-s)^2(\varepsilon eL-v)$$
$$+\left(a^2(b+1)^2(2\varepsilon eL+L-2v) - 2c\varphi(a+2\varepsilon e)(1-s)\right)\theta^2$$
$$+\theta\left(c^2\varphi^2(1-s)^2(a^2+\varepsilon e)L + a^4(b+1)^4L^3 - (1-s)a^2(b+1)^2(2aL+4\varepsilon e+c\varphi v)\right)\Big) - \widetilde{\pi_I^*}$$

。MSSP 的预期收益为 $\widetilde{\pi_{II}^{M*}} = \dfrac{1}{4a^2(b+1)^2\theta L + 2c\varphi(1-s)}\Big(a^2(b+1)^2L^2\left(\theta^2(4\varepsilon e+1)+1\right) - 2Lc\varphi(a+\varepsilon e)(1-s)$
$+2\left(c\varphi L(1-s)(a+\varepsilon e-a^2) - a^2(b+1)^2L^2(2e\varepsilon+1)\right)\Big) - \widetilde{\pi_I^*}$。

通过引理 3 可以发现，由于无法验证 MSSP 的安全质量，虽然 MSSP 可以提供一个较好的安全水平来保障企业的信息安全，但是 MSSP 也会提供比标准更低的安全质量。

4. 均衡分析

4.1. 敏感性分析

首先，对不同安全标准水平下的最优决策进行分析，可以发现安全补贴系数与安全质量和赔偿费用之间的关系如定理 1 所示。

定理 1：(a) 企业和 MSSP 提供的安全质量会随着安全补贴系数的增加而增加，即 $\dfrac{\partial q_I^*}{\partial s} > 0$，$\dfrac{\partial q_{II}^*}{\partial s} > 0$；

(b) MSSP 的赔偿费用随着安全补贴系数的增加而减少，即 $\dfrac{\partial d_{II}^*}{\partial s} < 0$。

证明：对安全质量求导得：$\frac{\partial q_I^*}{\partial s}=\frac{aL\left(1-\theta+2a\theta\right)c}{\left(2\theta La^2\left(b+1\right)^2+c\left(1-s\right)\right)^2}>0$，$\frac{\partial q_{II}^*}{\partial s}=\frac{aL\left(1-\theta+2a\theta\right)\varphi c}{\left(2\theta La^2\left(b+1\right)^2+c\varphi\left(1-s\right)\right)^2}>0$，对 MSSP 的赔偿费用求导得：$\frac{\partial d_{II}^*}{\partial s}=-\frac{\left(1-\theta+2a\theta\right)a^2\left(b+1\right)^2L^2c\varphi\theta}{\left(2\theta La^2\left(b+1\right)^2+c\varphi\left(1-s\right)\right)^2}<0$。

定理 1(a)表明安全补贴系数对企业的信息安全水平有着积极的作用。随着安全补贴系数的增加，企业的 MSSP 的安全成本也在不断降低，较低的安全成本让企业和 MSSP 更愿意投入安全措施来提高企业的安全水平。定理 1(b)表示政府给予安全补贴越高，MSSP 就会提供一个较低的赔偿费用。因为较高的安全水平会降低企业发生信息安全事件的概率，安全损失也会降低，因为 MSSP 倾向于提供一个较低的赔偿费用。

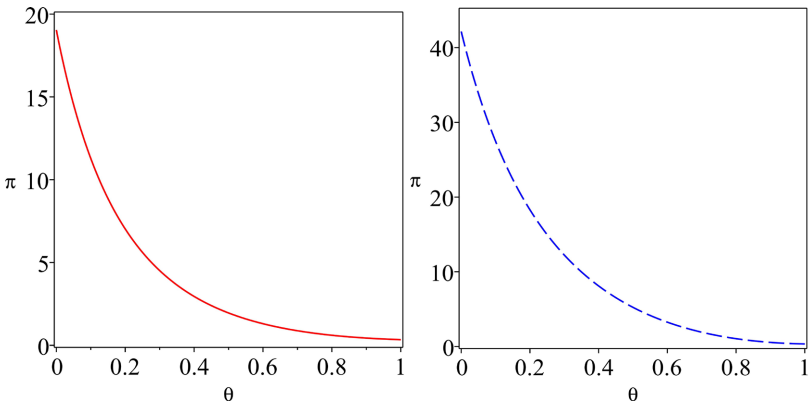
其次，我们对资产互补程度和企业的收益进行分析得到定理 2。

定理 2：无论安全标准的大小，企业选择内部管理安全时，企业的收益会随着信息资产互补程度的增加而增加，即 $\frac{\partial \pi_I^*}{\partial \theta}>0$，$\frac{\partial \widetilde{\pi_I^*}}{\partial \theta}>0$。

证明：对企业在宽松安全标准下的收益求导得

$\frac{\partial \pi_I^*}{\partial \theta}=\frac{aL\left(a^2L\left(1+\theta\right)+\left(1-a\right)\left(1-s\right)c\right)\left(\left(1-s\right)c-aL\left(1-\theta\right)\right)}{\left(2a^2\theta L+c-cs\right)^2}$，由约束条件 $L<\frac{\left(1-s\right)c}{a\left(1-\theta\right)}$ 可得 $\left(1-s\right)c-aL\left(1-\theta\right)>0$，所以 $\frac{\partial \pi_I^*}{\partial \theta}>0$。同理，对企业在严格安全标准下的收益求导，可得 $\frac{\partial \widetilde{\pi_I^*}}{\partial \theta}=\left(1-q_0\right)aL\left(1-a+aq_0\right)>0$。

从定理 2 可知，当企业选择在内部管理时，无论安全标准是否严格，随着互补程度的增加，企业的预期收益都会增加。因为发生信息安全事件时，互补企业的安全损失也会随着互补程度的增加而减少（$p_i\left(1-p_j\right)\left(1-\theta\right)L+p_ip_jL$），黑客能从企业获得的价值也降低，所以企业的收益会随着互补程度的增加而增加。此外，在外包情境下，研究互补程度与 MSSP 的收益之间的确定性关系在难以进行的。我们利用数值仿真得到外包情景下互补程度与MSSP收益的关系如图1所示，并总结结论在观察1，其中 $L=40$，$c=10$，$v=10$，$\varphi=0.7$，$a=0.2$，$\varepsilon=0.1$，$e=0.1$，$b=-0.1$，$s=0.6$。



(a) 宽松安全标准下　　(b) 严格安全标准下

Figure 1. MSSP's excepted payoff with θ under different security standards

图 1. 不同安全标准下 MSSP 预期收益与 θ 的关系

观察 1：无论安全标准的大小，MSSP 的收益会随着互补程度的增加而减少。

观察 1 表明，在外包情境下，随着互补程度的增加，MSSP 的收益会随着减少。从定理 2 中可以发现，企业的收益会随着互补程度的增加而增加，因此企业在外包时获得保留效益也会增加。MSSP 不得不给企业提供更高的保留效益来吸引客户企业，自身的收益也会降低。因此，过高的互补程度会降低 MSSP 的收益。接下来，我们还讨论了企业和 MSSP 的收益和安全补贴系数之间的关系，如定理 3 所示。

定理 3：无论安全标准是否严格，企业选择自我管理时，企业的收益会随着安全补贴系数的增加而增加，即 $\frac{\partial \pi_I^*}{\partial s}>0$，$\frac{\partial \widetilde{\pi_I^*}}{\partial s}>0$；

证明：对企业在宽松和严格安全标准下的收益分别求一阶导，可得 $\frac{\partial \pi_I^*}{\partial s}=\frac{a^2cL^2\left(1-\theta+2a\theta\right)^2}{2\left(c-cs+2a^2\theta L\right)^2}>0$，$\frac{\partial \widetilde{\pi_I^*}}{\partial s}=\frac{1}{2}cq_0^2>0$。

从定理 3 中可以看出，企业的收益总是会随着安全补贴系数的增加而增加，这有两个方面的原因。在一方面，从定理 1(a)可知，安全补贴系数的增加，企业的安全质量也会增加，企业的预期损失也会减小，安全损失的降低会对企业的收益产生正面的影响。在另一方面，由于安全补贴系数的增加，企业利用安全措施的成本也会降低。因此，企业的预期收益会随着安全补贴系数的增加而降低。

同理，在外包情境下，MSSP 的收益与安全补贴系数的关系如定理 4 所示。

定理 4：当两个企业选择外包时，

(a) 当安全标准宽松时，MSSP 的收益都会随着安全补贴系数的增加先增加后减少，即当 $0<s<s'$ 时，$\frac{\partial \pi_{II}^*}{\partial s}>0$，否则，$\frac{\partial \pi_{II}^*}{\partial s}<0$；

(b) 当安全标准严格时，MSSP 的收益会随着安全补贴系数的增加先减少后增加，即当 $0<s<s''$ 时，$\frac{\partial \widetilde{\pi_{II}^*}}{\partial s}<0$，否则，$\frac{\partial \widetilde{\pi_{II}^*}}{\partial s}>0$。

证明：对外包情况下，当安全标准宽松时，对 MSSP 的预期收益求一阶导，可得 $\frac{\partial \pi_{II}^*}{\partial s}=\frac{\left(b^2+2b+1-\varphi\right)\left(4\left(b+1\right)^2a^4\theta^2L^2-c^2\left(1-s\right)^2\varphi\right)L^2\left(1-\theta+a\theta\right)^2a^2c}{2\left(4a^2\left(b+1\right)^2-c\left(1-s\right)^2\varphi\right)^2\left(4a^2\theta L-\left(1-s\right)c\right)^2}$，通过对 $\frac{\partial \pi_{II}^*}{\partial s}=0$ 求解，可得 $s'=1-\frac{2a^2\theta L\sqrt{\varphi}}{c\varphi}$(其中另一个解 $1+\frac{2a^2\theta L\sqrt{\varphi}}{c\varphi}$ 明显大于 1，不符合安全补贴系数 $s\in[0,1]$ 的取值范围，故舍去)。当 $s>s'$ 时，$\frac{\partial \pi_{II}^*}{\partial s}>0$，当 $s<s'$ 时，$\frac{\partial \pi_{II}^*}{\partial s}<0$。同理，当安全标准严格时，对 MSSP 的预期收益求一阶导并求解，得 $s''=1-\frac{aL\left(b+1\right)\left(1-\theta+2a\theta\right)\sqrt{\varphi}-2a^2\left(b+1\right)^2\theta Lq_0}{q_0c\varphi}$。当 $s>s''$ 时，$\frac{\partial \widetilde{\pi_{II}^*}}{\partial s}>0$，当 $s<s''$ 时，$\frac{\partial \widetilde{\pi_{II}^*}}{\partial s}<0$。

定理 4 表示在外包情境下，当安全标准宽松时，MSSP 的收益会随着安全补贴系数的增加先增加后减少，但是当安全标准比较严格时，情况则恰恰相反，MSSP 的收益会随着安全补贴系数的增加先减少后增加。安全标准的范围会对 MSSP 的收益产生的不同的影响。

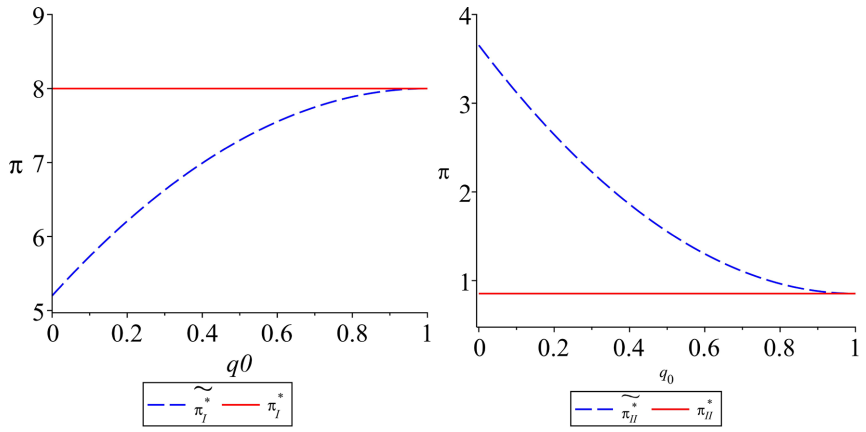
随后，研究还发现不同的安全标准会对企业和 MSSP 的收益产生不同的影响，如定理 5 所示。

定理 5：(a) 当安全标准宽松时，安全标准对企业和 MSSP 的收益没有影响；

(b) 当安全标准严格时，企业的收益会随着安全标准的增加而减少，MSSP 的收益会随着安全标准的增加而增加。

证明：当安全标准宽松时，两种安全情景下，企业和 MSSP 的均衡结果不变，此时企业和 MSSP 的收益与安全标准无关。当安全标准严格时，$\frac{\partial \widetilde{\pi}_I^*}{\partial q_0}=a\left(1-\theta+2a\theta\left(1-q_0\right)\right)-cq_0\left(1-s\right)$，$\frac{\partial^2 \widetilde{\pi}_I^{*2}}{\partial^2 q_0}=-2La^2\theta-\left(1-s\right)c$，所以 $\frac{\partial \widetilde{\pi}_I^*}{\partial q_0}$ 是一个关于 q_0 的递减函数，且驻点 $\frac{aL\left(2a\theta-\theta+1\right)}{2a^2L\theta+\left(1-s\right)c}$ 处值小于 0，因此 $\frac{\partial \widetilde{\pi}_I^*}{\partial q_0}<0$。同理，$\frac{\partial \widetilde{\pi}_{II}^*}{\partial q_0}=-a\left(1-\theta+2a\theta\left(1-q_0\right)\right)+cq_0\left(1-s\right)$，$\frac{\partial^2 \widetilde{\pi}_{II}^{*2}}{\partial^2 q_0}=2La^2\theta+\left(1-s\right)c$，所以 $\frac{\partial \widetilde{\pi}_{II}^*}{\partial q_0}$ 是一个关于 q_0 的递减函数，且驻点 $\frac{aL\left(2a\theta-\theta+1\right)}{2a^2L\theta+\left(1-s\right)c}$ 处值大于 0，因此 $\frac{\partial \widetilde{\pi}_I^*}{\partial q_0}>0$。

定理 5(a)表明当安全标准宽松时，企业和 MSSP 的预期收益与安全标准的大小无关。因为宽松的安全标准低于企业和 MSSP 的均衡结构，对内部管理企业和 MSSP 的预期收益没有影响。但是，定理 5(b)表示安全标准过高时，会损害企业的预期收益但是有利于 MSSP 获得更高的收益。当安全标准过高时，企业由于审查必须提供如标准要求一致的安全质量，而过高的安全质量虽然提高了企业的安全水平，但也带来投资风险造成过高的安全投入，企业的预期收益会随着安全标准的增加而减少。与此相反，MSSP 由于它的安全质量的不可验证性，MSSP 虽然声称会达到安全标准要求的安全质量，但是实际上并没有如实提供，MSSP 的收益会随着安全标准的增加而增加。图 2 展示了企业和 MSSP 的收益如何随着安全标准的变化而变化的数值仿真，其中 $L=40$，$c=10$，$v=10$，$\varphi=0.7$，$\theta=0.5$，$a=0.2$，$\varepsilon=0.1$，$e=0.1$，$b=-0.1$，$s=0.6$。



(a) 企业收益　　(b) MSSP 收益

Figure 2. The relationship between payoff and mandatory security standards
图 2. 企业和 MSSP 收益与安全标准的关系

4.2. 最优决策比较

在本节，首先，通过比较不同安全标准下企业和 MSSP 收益之间的联系，如定理 6 所示。

定理 6：严格安全标准下的企业的预期收益小于宽松安全标准情况下的企业的预期收益，但是 MSSP 的预期收益却相反。即 $\pi_I^*>\widetilde{\pi}_I^*$，$\pi_{II}^*<\widetilde{\pi}_{II}^*$。

证明： 由 $\pi_I^* - \widetilde{\pi}_I^* = \frac{\left(aL\left(1-\theta+2a\theta\left(1-q_0\right)\right)-cq_0\left(1-s\right)\right)^2}{4a^2\theta L+2\left(1-s\right)c} > 0$ 可得 $\pi_I^* < \widetilde{\pi}_I^*$。

$\pi_{II}^* - \widetilde{\pi}_{II}^* = -\frac{\left(aL\left(1-\theta+2a\theta\left(1-q_0\right)\right)-cq_0\left(1-s\right)\right)^2}{4a^2\theta L+2\left(1-s\right)c} < 0$ 可得 $\pi_{II}^* > \widetilde{\pi}_{II}^*$。

定理 6 表明，严格的安全标准会损害企业的收益，但是可以给 MSSP 带来更高的收益。当安全标准宽松时，企业会提供均衡下的最优安全质量，当安全标准严格时，企业不得不提高安全质量来达到要求的安全标准。过高的安全标准虽然会提高企业的安全水平但是也让企业的安全成本增加，企业的收益相较于宽松安全标准时的收益会变少。当企业选择将安全外包给 MSSP 时，更严格的安全标准有利于 MSSP 获得更高的收益。因为安全标准不会改变 MSSP 的均衡安全质量，当安全标准宽松时，MSSP 的均衡安全质量超过标准，MSSP 会如实提供 BRC 中规定的安全质量，当安全标准严格时，MSSP 会声称自己提供安全质量 q_0，但是实际上只会提供均衡安全质量 q_{II}^*，因此 MSSP 会获得更高的收益。

接下来，对社会福利进行比较可以得到定理 7。

定理 7：(a) 当两个企业选择自我管理，过于严格的安全标准会降低社会福利；

(b) 当两个企业选择外包时，安全标准的并不影响社会福利。

证明：当企业都选择自我管理时，安全标准宽松时，此时社会福利可以表示为：$SW_{in-house} = 2\pi_I^*$。当安全标准严格时，社会福利可以表示为：$SW'_{in-house} = 2\widetilde{\pi}_I^*$，

$SW'_{in-house} - SW_{in-house} = \frac{\left(aL\left(1-\theta+2a\theta\left(1-q_0\right)\right)-cq_0\left(1-s\right)\right)^2}{4a^2\theta L+2\left(1-s\right)c} < 0$，可得 $SW'_{in-house} < SW_{in-house}$。当企业选择外包给 MSSP 时，当安全标准宽松和严格时，社会福利可分别表示为：$SW_{out} = 2\pi_I^* + \pi_{II}^*$，$SW'_{out} = 2\widetilde{\pi}_I^* + \widetilde{\pi}_{II}^*$，并且 $SW'_{out} - SW_{out} = 0$，由此可以推出 $SW'_{out} = SW_{out}$。

证毕。

定理 7(a)表明过高的安全标准会损害社会福利，出现这种结论是并不意外，如果安全标准超过企业自我管理时的均衡质量，那么企业不得不加大对信息安全的投入如购买有关设备、加强员工的安全培训来达到规定的安全标准，此时企业的安全成本会增加，这种额外的努力对于社会而言是多余的。相反地，定理 7(b)表示无论安全标准是宽松还是严格，对外包情景下的社会福利并不会产生影响，虽然 MSSP 声称会提供合同中所规定的安全质量，但是由于 MSSP 的安全努力无法得到验证，MSSP 也不会做额外的安全努力，安全标准不会影响 MSSP 提供给企业的安全质量，只会影响 MSSP 获得的预期收益，但是社会福利并没有发生变化。因此，从定理 7 中可以得到一些管理启示，企业选择自我管理时，过于严格的安全标准对社会规划者而言并不是最优的方案，政府部门应仔细衡量安全标准给企业带来的投资成本。而企业选择外包时，从社会福利的角度来看，对 MSSP 的安全努力进行审查和验证是不被建议的。

4.3. 最优策略选择

本节主要研究了互补企业在不同安全条件下的最优安全策略选择。首先，本节对外包情景下存在的信息泄露风险进行研究得到定理 8 如下。

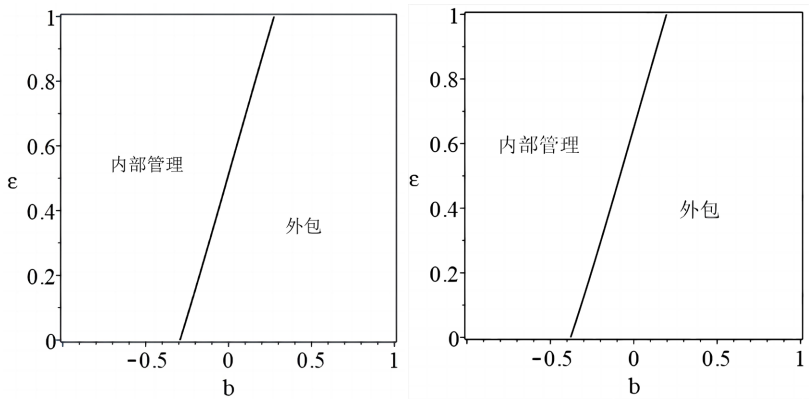
定理 8：无论安全标准是否严格，当信息泄露小于一定阈值时，MSSP 才愿意服务企业，但是安全标准过于严格时，信息泄露风险的负面影响会得到削弱。即当 $\varepsilon < \varepsilon'$ 时，$\pi_{II}^* > 0$，当 $\varepsilon < \varepsilon''$，$\widetilde{\pi}_{II}^* > 0$，并且 $\varepsilon' < \varepsilon''$。

证明：通过求解 $\pi_{II}^* = 0$，可得 $\varepsilon' = \frac{a^2cL\left(1-s\right)\left(1-\theta+2a\theta\right)^2\left(\left(b+1\right)^2-\varphi\right)}{2e\left(2a^2\left(b+1\right)^2\theta L+\left(1-s\right)c\varphi\right)\left(1-\theta\right)\left(2a^2\theta L+\left(1-s\right)c\right)}$。所以当 $\varepsilon < \varepsilon'$

时，$\pi_{II}^{*}>0$。通过求解$\widetilde{\pi_{II}^{*}}=0$，可得

$\varepsilon''=\dfrac{a^2(b+1)^2L^2(1-\theta-2a\theta(1-q_0))^2-(1-s)^2c^2q_0^2\varphi+2q_0(1-s)acL\left(\left(a\left((b+1)^2q_0-2\varphi\right)+\varphi\right)\theta-\varphi\right)}{(1-\theta)eL\left(2a^2(b+1)^2\theta L+c\varphi(1-s)\right)}$。所以当$\varepsilon<\varepsilon''$时，$\widetilde{\pi_{II}^{*}}>0$。对两个阈值进行比较，得到$\varepsilon''-\varepsilon'=\dfrac{\left((1-s)cq_0-aL(1-\theta+a\theta(1-q_0))\right)^2}{2\left(2a^2\theta L+(1-s)c\right)(1-\theta)eL}>0$。所以可以得出$\varepsilon'<\varepsilon''$。

定理 8 表明无论是否有安全补贴和安全标准，只有在信息泄露风险低于一定阈值时，MSSP 才愿意进行信息安全市场为客户企业提供安全服务，并且过高的安全标准会削弱信息泄露风险的劣势。值得注意的是，当安全标准更为宽松时，信息泄露风险的劣势会得到进一步加强，MSSP 会对信息泄露风险变得更为敏感。接下来，我们采用了数据仿真来确定在不同安全标准下，企业内部管理和外包情境下 MSSP 的最优决策，如图 3 所示，其中$e=0.1$，$a=0.2$，$\theta=0.5$，$\varphi=0.5$，$L=20$，$c=10$，$q_0=0.8$。



(a) 宽松安全标准下的最优策略选择　(b) 严格安全标准下的最优策略选择

Figure 3. The optimal scenario under different security standard
图 3. 不同安全标准下的最优策略选择

观察 2：当安全标准过于严格时，MSSP 更倾向于选择为客户企业提供安全服务。

从观察 2 中，可以总结出几个重要的结论：首先，MSSP 在为客户企业提供服务时，会在信息泄露风险和安全外部性中进行权衡，研究发现当安全外部性为负且信息泄露风险较低时，MSSP 愿意为客户企业提供服务，虽然负安全外部性会增加企业发生信息安全事件的概率，但是 MSSP 可以从客户企业处获得更大的收益。其次，从图 3 中可以发现随着正的安全外部性增加，企业选择内部管理的区块仍然存在，这表明当信息泄露风险的劣势很大，企业不太愿意将安全外包给 MSSP，尽管 MSSP 具有成本效益和正安全外部性的优势。最后，对比图 3(a)和图 3(b)的区块，可以发现当安全标准过于严格时，MSSP 端信息泄露风险劣势得到进一步的削弱，MSSP 也更倾向于为客户企业提供安全服务。

5. 结论与展望

本文以互补企业作为研究基础，考虑有安全标准和安全补贴时，两个互补企业内部自我管理和外包给 MSSP 两种情景下的信息安全决策。通过研究发现，由于 MSSP 的努力的不可验证性，MSSP 可能会逃避责任，但是这种逃避并不一定会带来负面影响，也给安全管理提供了一定的管理启示。

首先，本文发现互补企业的互补程度可以有效地降低企业在安全事件中的遭受的损失从而提高企业

的收益，但是 MSSP 的收益会随着互补程度的增加而降低，因为互补的信息资产性质降低了企业在发生安全事件时遭受的损失。其次，本文发现无论是内部管理还是安全外包，随着安全补贴的增加，企业和 MSSP 都会提高安全质量。但是随着安全标准的增加，企业会选择将安全外包给 MSSP 来逃避责任，即使企业知道 MSSP 不会如实提供标准一致的安全质量，并且内部管理时，过高的标准会损害社会福利。接着，本文发现强制安全标准和安全补贴系数会对企业和 MSSP 的均衡收益产生不同的影响，当强制安全标准较为宽松时，MSSP 的收益都会随着安全补贴系数的增加先增加后减少，当强制安全标准较为严格时，MSSP 的收益都会随着安全补贴系数的增加先减少后增加。最后，本文发现 MSSP 会在信息泄露风险和安全外部性之间做权衡，只有在信息泄露风险低于一定阈值时才愿意服务企业，当强制安全标准过高时，信息泄露风险的劣势会得到削弱，MSSP 会更倾向于为客户企业提供服务。

虽然通过研究得到了一些结论和启示，但是在未来可以从以下方面入手进行拓展研究：首先，本文在考虑企业面临安全环境时，没有考虑战略黑客对于企业安全水平的影响，未来可以将策略黑客纳入研究范围，考虑黑客行为对于信息决策的影响；其次，本文研究是基于同质企业进行的，没有考虑到异质企业不同损失对研究的影响，未来可以将异质企业的影响纳入研究范围内。

参考文献

[1] Statista (2020) Managed Security Services Market Size Worldwide in 2020 and 2026. https://www.statista.com/statistics/1230718/managed-security-services-market-it/

[2] Zhao, X., Xue, L. and Whinston, A.B. (2013) Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements. *Journal of Management Information Systems*, **30**, 123-152. https://doi.org/10.2753/MIS0742-1222300104

[3] Ulltveit-Moe, N. (2014) A roadmap towards Improving Managed Security Services from a Privacy Perspective. *Ethics and Information Technology*, **16**, 227-240. https://doi.org/10.1007/s10676-014-9348-3

[4] 吴勇, 王林萍, 冯耕中. 双边道德风险下供应链互补企业信息安全外包激励契约研究[J]. 系统工程理论与实践, 2022, 42(11): 2916-2926.

[5] Liu, D., Ji, Y. and Mookerjee, V. (2011) Knowledge Sharing and Investment Decisions in Information Security. *Decision Support Systems*, **52**, 95-107. https://doi.org/10.1016/j.dss.2011.05.007

[6] UK G (2022) National Cyber Strategy 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

[7] 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

[8] Wu, Y., Fung, R.Y.K., Feng, G., *et al*. (2017) Decisions Making in Information Security Outsourcing: Impact of Complementary and Substitutable Firms. *Computers & Industrial Engineering*, **110**, 1-12. https://doi.org/10.1016/j.cie.2017.05.018

[9] Li, X. (2020) Decision Making of Optimal Investment in Information Security for Complementary Enterprises Based on Game Theory. *Technology Analysis & Strategic Management*, **33**, 755-769. https://doi.org/10.1080/09537325.2020.1841158

[10] Qian, X., Yang, W., Pei, J., *et al*. (2021) A Game of Information Security Investment Considering Security Insurance and Complementary Information Assets. *International Transactions in Operational Research*, **29**, 1791-1824. https://doi.org/10.1111/itor.12972

[11] Ross, R. (2007) Managing Enterprise Security risk with NIST Standards. *Computer*, **40**, 88-91. https://doi.org/10.1109/MC.2007.284

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

[13] Lee, C.H., Geng, X. and Raghunathan, S. (2013) Contracting Information Security in the Presence of Double Moral Hazard. *Information Systems Research*, **24**, 295-311. https://doi.org/10.1287/isre.1120.0447

[14] 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

[15] 赵柳榕，刘健楠，朱晓峰. 竞争企业的信息安全策略选择:自主防御或外包[J]. 情报理论与实践，2019(42): 94-100+159.

[16] Feng, N., Chen, Y., Feng, H., *et al*. (2020) To Outsource or Not: The Impact of Information Leakage Risk on Information Security Strategy. *Information & Management*, **57**, Article ID: 103215. https://doi.org/10.1016/j.im.2019.103215

[17] Wu, Y., Tayi, G.K., Feng, G., *et al*. (2021) Managing Information Security Outsourcing in a Dynamic Cooperation Environment. *Journal of the Association for Information Systems*, **22**, 827-850. https://doi.org/10.17705/1jais.00681

[18] Hui, K.-L., Hui, W. and Yue, W.T. (2012) Information Security Outsourcing with System Interdependency and Mandatory Security Requirement. *Journal of Management Information Systems*, **29**, 117-156. https://doi.org/10.2753/MIS0742-1222290304

[19] Lee, C.H., Geng, X. and Raghunathan, S. (2016) Mandatory Standards and Organizational Information Security. *Information Systems Research*, **27**, 70-86. https://doi.org/10.1287/isre.2015.0607

[20] Hui, K.-L., Ke, P.F., Yao, Y., *et al*. (2019) Bilateral Liability-Based Contracts in Information Security Outsourcing. *Information Systems Research*, **30**, 411-429. https://doi.org/10.1287/isre.2018.0806

[21] Gao, X., Gong, S., Wang, Y., *et al*. (2022) An Economic Analysis of Information Security Decisions with Mandatory Security Standards in Resource Sharing Environments. *Expert Systems with Applications*, **206**, Article ID: 117894. https://doi.org/10.1016/j.eswa.2022.117894

[22] 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): 70-81.

[23] Avasant (2009) Use of IT Security Outsourcing Low but Rising as Threats Grow. https://avasant.com/report/it-security-outsourcing-still-small-but-promising/