Management Science and Engineering 管理科学与工程, 2023, 12(1), 1-18
Published Online January 2023 in Hans. https://www.hanspub.org/journal/mse
https://doi.org/10.12677/mse.2023.121001

Hans汉斯

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

刘艺浩，吴　勇

东华大学旭日工商管理学院，上海

收稿日期：2022年12月17日；录用日期：2023年1月7日；发布日期：2023年1月19日

摘　要

信息技术的快速发展不仅方便了人们的生活，同时也给企业和个人带来了更大的安全隐患。为了应对安全风险的挑战，企业倾向于将部分信息安全外包给专业的管理安全服务提供商(MSSP)，MSSP旨在通过专业高效的信息安全管理手段来帮助企业提高信息安全质量。因此，本文考虑了部分外包发生时企业和MSSP之间不对称的安全外部性以及强制性安全标准约束，探究了企业的两种部分外包策略(核心外包策略和非核心外包策略)，为企业的安全实践提供了管理启示。我们发现，当企业对MSSP的外部性为负(正)时，在较低的安全标准下，企业付出的安全努力水平总是随着MSSP对企业外部性的增大而增大(减小)。另外，我们发现不同程度的强制性安全标准对企业和MSSP最优决策的影响不同。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，企业需设定赔偿比例从而得到最低期望成本；然而，在较高的强制性安全标准约束下，企业无需设立赔偿机制即可达到最优决策。此外，当信息泄露风险较高时，企业总是选择非核心外包策略。

关键词

部分外包，安全外部性，信息泄露，强制性安全标准

Managing Partial Outsourcing on Information Security under Security Standard Constraint

—Based on Asymmetric Externality

Yihao Liu, Yong Wu

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

Received: Dec. 17th, 2022; accepted: Jan. 7th, 2023; published: Jan. 19th, 2023

文章引用: 刘艺浩, 吴勇. 安全标准约束下的信息安全部分外包研究[J]. 管理科学与工程, 2023, 12(1): 1-18.
DOI: 10.12677/mse.2023.121001

Abstract

The rapid development of information technology has not only greatly facilitated people's lives, but also brought greater security risks for firms. In order to meet the challenges of security risks, the firm often chooses to outsource partial information security to a professional managed security service provider (MSSP), which aims to improve the quality of information security through professional and efficient information security management means. Therefore, this paper considers the asymmetric security externality between the firm and the MSSP and the mandatory security standard constraint when partial outsourcing occurs to explore two partial outsourcing strategies, that is, Core Outsourcing Strategy (OC Strategy) and Non-core Outsourcing Strategy (ONC Strategy), and the research results can provide management insights for the firms' security practice. We find that when the firm's externality to the MSSP is negative (positive), the firm's security effort always increases (decreases) as the MSSP's externality to the firm increases under loose security standards. In addition, we find that different levels of mandatory security standards have different effects on the optimal decision of the firm and MSSP. When the firm adopts OC Strategy, the firm needs to set a compensation ratio to get the minimum expected cost under loose mandatory security standards. However, the firm can reach the optimal decision without setting up the compensation mechanism under stricter mandatory security standards. Besides, the firm always chooses the ONC Strategy when the information leakage risk is higher.

Keywords

Partial Outsourcing, Security Externality, Information Leakage, Mandatory Security Standard

1. 引言

近年来信息技术发展迅速并得到了广泛应用，信息技术的发展极大地方便并丰富了人们的生活，但与此同时信息安全事件也屡出不穷，给经济社会带来了严重影响。根据《2021 年中国网络安全报告》[1]，2021 年一年内瑞星云安全系统截获网络病毒样本、恶意网址、病毒感染次数总计高达 4.41 亿次。2021 年 4 月，勒索软件恶意攻击加拿大无线设备制造商的 IT 系统，导致 Sierra 在全球各地的生产基地停产[2]。2022 年 4 月，北美国家哥斯达黎加财政部证实被 conti 勒索软件攻击，无数敏感数据被盗，窃取纳税人信息引起了公共恐慌[3]。此一系列网络安全事件给人们生产生活带来了巨大威胁。

为了预防黑客攻击，并降低黑客攻破信息系统带来的安全损失，许多企业倾向于将其业务安全外包给专业的托管安全服务提供商(Managed Security Service Provider，以下简称为 MSSP)。据报道，到 2025 年，托管安全服务市场价值 464 亿美元[4]。在实践中，由于信息安全外包行业存在信息泄露风险，将部分信息业务外包给 MSSP 的情况较为普遍。Cybersecurity insiders 的报告显示，91%的企业担心云安全服务商的数据泄露问题，比起外包给 MSSP，企业更愿意把核心数据储存在内部[5]。尤其是近年来大型云安全服务商的数据泄露事故层出不穷，加剧了企业对于云安全的担心。例如，2021 年 2 月，新加坡知名电信公司新电信(Singtel)在其官网发布消息称，由第三方供应商(Accellion)提供的文件共享系统 FTA 被身份未知的黑客非法攻击，导致数据泄露[6]。信息泄漏源于业务信息从企业到 MSSP 的转移，可能发生在

检测和分析过程中[7]。因此，在安全外包实践中，企业往往会选择将部分业务安全外包给 MSSP 而非全部外包。在实践中，企业通常将其业务分为核心和非核心业务，其中核心业务是为企业创造重大价值的关键部分，对企业绩效、潜在竞争优势和未来增长至关重要[8]。先前的研究表明，对于 IT 企业而言，部分外包的成功率高于全部外包或全部自主管理[9]。

值得注意的是，当部分外包发生时，由于管理主体的增加，企业和 MSSP 付出的安全努力，即对应管理业务的安全质量，将通过安全外部性相互影响[10]。安全外部性意味着，为保护或攻击一个主体所付出的努力可能会影响其他主体的安全水平。安全外部性带来的影响可能是积极的或者消极的[11]。积极的外部性，即正外部性的一个例子是，当企业将部分业务外包给 MSSP 时，双方将建立合作关系，并相互学习信息安全技术，从而更好地保护其业务。此外，当黑客战略性地选择薄弱目标时，就会产生消极的外部性，即负外部性：在一个攻击目标具有更强有力的安全保护的情况下，黑客可能会将注意力转移到安全级别相对较低的其他目标，我们称之为“攻击转移”[10] [12]。此外，由于企业和 MSSP 运营性质的不同，企业对 MSSP 的外部性和 MSSP 对企业的外部性往往是不对称的。因此，在安全外部性影响下企业应如何制定安全运营策略，值得深入研究。

此外，强制性安全标准也是影响信息安全投资的另一个关键因素。安全标准作为建设信息安全保障体系的重要支撑，是保证企业最低安全投入的重要工具，可以从社会监管机构或行业协会的角度提高信息系统的安全水平。一般而言，安全要求的目的不仅是区别地保护政府、机构和个人拥有的信息资产，而且还保护存储、传输和处理这些信息资产的信息系统。在此基础上，对不同安全要求的信息安全响应进行了区分处理。企业和其他组织的信息安全要求可以单独制定，以更好地保护其自身的信息资产[13]。

综上所述，信息安全问题已经引起个人和企业的高度重视。为了将安全损失最小化，企业通常需要考虑信息泄露、安全外部性、强制性安全标准三重因素进行信息安全管理方面的投资决策研究。本文考虑了企业的两种部分外包策略，一是将核心业务外包给 MSSP，非核心业务由企业内部管理(OC 策略)，二是将非核心业务外包给 MSSP，核心业务由企业内部管理(ONC 策略)，进而探究了企业在不同环境下的信息安全管理策略，为企业的安全实践提供参考。

2. 文献综述

本文的文献研究主要涉及以下几个领域：信息安全部分外包、安全外部性及强制性安全标准。

目前，对部分外包的研究主要集中在运营管理领域。Grossman (2005) [14]表明国际外包的程度外取决于供应商国内外市场的厚度、在每个市场搜索的相对成本、定制投入品的相对成本以及每个国家合同环境的性质。Shy 和 Stenbacka (2005) [15]调查竞争如何影响生产分包投入的比例并得出结论：外包投入的比例随着竞争的增强而增加。Alvarez 和 Stenbacka (2007) [16]运用实物期权方法对企业的最优组织模式进行一般性描述，并得出结论：建立部分外包的最佳阈值是潜在市场不确定性的一个不断增加的函数。然而在信息安全领域，关于部分外包的研究却很少。以往大多数关于信息安全外包的文献认为，企业选择是将其信息安全全部外包给 MSSP 或采用内部管理策略，而忽略将部分外包作为一种替代战略。然而在实践中，企业通常将其部分安全功能外包，以有效地管理信息安全。企业通常专注于高效利用自己的资源，同时支付 MSSP 以执行他们不太擅长的功能并避免专有信息被盗[17] [18]。Cezar 等(2014) [19]将 MSSP 的功能归类为预防和检测，他们发现预防和检测功能在合同层面上是相互依赖的。Yang 等(2020) [20]研究了当用户外包部分云安全管理时，云服务模型对供应商和用户激励措施的影响。本文与上述研究的不同之处在于，我们将安全外部性作为影响企业和 MSSP 安全决定的关键因素，并对 OC 和 ONC 四种部分外包策略进行了比较。

目前关于安全外部性的研究相对较少。Lee 等(2013) [10]研究了 MSSP 和企业如何在企业侧外部性和

MSSP 侧外部性下协调努力以获得更好的安全性，他们提出了一种新的合同，称为多边合同，以解决双重道德风险问题。Zhao 等(2014) [21]将 MSSP 作为一种风险管理工具，表明服务于多个企业的 MSSP 可以将安全投资的外部性内化，并降低安全投资的低效率。Wu 等(2018) [22]考虑了竞争和整合环境下两个企业安全投资之间的外部性，并从三个维度对决策进行了比较竞争环境和整合环境之间的差异、正安全外部性和负安全外部性之间的差异以及企业间信息共享之间的差异。Zhang 等(2020) [23]得出结论，如果建立了商业伙伴关系的两家企业外包给同一家 MSSP，则两家企业的安全投资在正外部性下更大，反之亦然。Wu 等(2022) [24]考虑了企业之间的信息共享和风险相关性，并发现风险相关性激励企业共享安全知识。

由于安全标准作为一种管理信息安全的策略是最近才发展起来的，因此现有的关于该主题的研究有限。Miller 和 Tucker (2010) [25]表明，由于违反通知条例中的安全港规定，采用加密软件会增加公开数据丢失的事件部分原因是由于应保护信息资产的人对其他保护活动的疏忽。随着政府和行业协会对网络安全的高度重视，越来越多的学者致力于研究强制性安全标准对企业信息安全投资的影响。Ghose 和 Rajan (2006) [26]考虑了监管信息公开对企业安全投资的经济影响，因此强制性安全公开可以激励企业做出最佳生产决策。Lee 等(2016) [27]研究了强制性安全标准对企业最优安全决策的影响，并得出结论，更高的安全标准不一定导致更高的安全水平。Gao 等(2022) [28]研究表明，严格的强制性标准并不总是对每个企业都有利，即使其信息系统可以得到更好的保护。因此，应从社会最优的角度制定更严格的安全标准。此外，虽然补偿机制可以促使每个企业增加投资，但这种机制可能会损害每个企业。

基于上述文献综述，本文结合强制性安全标准、信息泄露和安全外部性对企业部分安全外包策略进行深入探究，这可以进一步丰富信息安全管理理论，为企业的安全实践提供管理启示。

3. 问题描述

在介绍基本模型之前，表 1 中收集了将在以下描述中出现的关键符号。

Table 1. Main notations
表 1. 主要模型符号

符号	参数说明
L_{NC}	黑客攻击非核心业务带来的安全损失
d	核心和非核心业务被黑客攻击导致安全损失的比例($d>1$)
η	单位成本系数比例($0<\eta<1$)
f_i	核心，非核心业务外包时的服务费($i\in\{C,NC\}$)
φ_i	MSSP 付给企业的赔偿比例($i\in\{C,NC\}$)
q_i^j	安全质量($i\in\{C,NC\}, j\in\{f,m\}, 0<q_i^j<1$)
α	信息泄露的可能性
ω	信息泄露和黑客攻击带来的安全损失的比例
β^{f2m}	企业的安全努力对 MSSP 的外部性
β^{m2f}	MSSP 的安全努力对企业的外部性
c_i	企业的成本系数($i\in\{C,NC\}$)
q_0	核心业务的强制性安全标准

我们考虑一个企业将其核心或非核心业务的安全管理外包给一个 MSSP，并面临确定最优信息安全管理策略的问题。本文根据企业经营实践，将企业业务分为核心业务和非核心业务。因此，企业可以选择两种类型的部分外包策略：1) 将核心业务外包给 MSSP，非核心业务由企业内部管理(OC 策略)；2) 将非核心业务外包给 MSSP，核心业务由企业内部管理(ONC 策略)。无论采用哪种策略，企业或 MSSP 都需要付出安全努力来提高企业业务的安全质量。我们用 q_i^j 表示相应业务的安全质量，该业务的安全质量可以通过企业或 MSSP 的安全努力来提高[1]。安全质量也代表在企业或 MSSP 的安全努力下，企业的业务能够阻止黑客攻击的概率。其中，$q_i^j \in (0,1)$ 因为 q_i^j 代表的是概率。当企业采用部分外包策略，即 OC 策略或 ONC 策略时，核心业务和非核心业务的安全质量由企业和 MSSP 分开管理。在这两种情况下，企业和 MSSP 的被攻击概率通过安全外部性关联。例如，当企业采用 OC 策略时，MSSP 在核心业务上的安全努力也会影响企业管理的非核心业务的攻击概率。由于企业和 MSSP 运营性质的不同，当企业和 MSSP 建立合作关系时，企业所付出的安全努力对 MSSP 安全努力的影响可能不同于 MSSP 安全努力对企业安全努力的影响。因此，我们将企业的安全努力对 MSSP 的外部性标记为 β^{f2m}，并在下面的描述中简称其为“f2m 外部性”；同时将 MSSP 安全努力对企业的外部性标记为 β^{m2f}，并在下面的描述中简称其为“m2f 外部性”。其中，β^{f2m} (β^{m2f})可以是正的，也可以是负的[29]。需要注意的是，当企业采用部分外包策略时，业务本身的安全质量在降低或增加业务被攻击概率方面占主导地位，因此，我们可以得到 $\beta^{f2m}, \beta^{m2f} \in (-1,1)$。

考虑到安全外部性，当企业采用 OC 策略时，核心业务和非核心业务被攻击的概率可以分别表示为 $p_C = 1 - q_C^m - \beta^{f2m} q_{NC}^f$ 和 $p_{NC} = 1 - q_{NC}^f - \beta^{m2f} q_C^m$。同样地，当企业采取 ONC 策略时，核心业务和非核心业务被攻击的概率可以分别表示为 $p_C = 1 - q_C^f - \beta^{m2f} q_{NC}^m$ 和 $p_{NC} = 1 - q_{NC}^m - \beta^{f2m} q_C^f$。表 2 列举了两种策略下不同业务被攻击的概率。

Table 2. Breach probability under two strategies
表 2. 两种策略下的攻击概率

攻击概率	核心业务	非核心业务
OC 策略	$p_C = 1 - q_C^m - \beta^{f2m} q_{NC}^f$	$p_{NC} = 1 - q_{NC}^f - \beta^{m2f} q_C^m$
ONC 策略	$p_C = 1 - q_C^f - \beta^{m2f} q_{NC}^m$	$p_{NC} = 1 - q_{NC}^m - \beta^{f2m} q_C^f$

安全措施的加强降低了企业被攻击的可能性，但这需要更多的成本。Gartner 报告称，大多数最初的安全防护涉及基本的基础设施技术(“阻止坏人进入”技术)，比如成本稳定的防火墙和反病毒技术，随后的保护重点转向了“让好人进入”技术，比如身份验证和访问管理。后者通常需要更多的配置和管理投资[30] [31]。因此，我们假设企业提高安全质量的努力成本是增加且是凸函数，即 $\frac{1}{2} c_i q_i^{j2}$，其中 c_i 是企业的单位成本系数。相应的，MSSP 的安全努力成本为 $\frac{1}{2} \eta c_i q_i^{j2}$ [23]，其中 η 为 MSSP 与企业的单位成本系数之比。由于 MSSP 在安全保护方面通常比企业更具有成本效益[32]。因此，我们假设 $\eta \in (0,1)$，随着 η 下降，MSSP 的成本效率更高。

在安全外包行业中，双边退款合同以服务水平协议的形式广泛应用于安全外包行业[33]。合同(f_i, φ_i) 指定企业需要支付服务费 f_i 给 MSSP，一旦企业遭受攻击，MSSP 需要赔偿企业 $\varphi_i L_i$，其中 φ_i 代表赔偿比例，dL_{NC} 和 L_{NC} 分别代表核心和非核心业务被黑客攻击带来的损失，其中 $d > 1$ 永远成立，意味着核心业务比非核心业务更重要，一旦被攻击带来的损失也更大。此外，企业在将业务外包给 MSSP 时，不仅

[1] $i \in \{C, NC\}$ 代表核心或非核心业务，$j \in \{f, m\}$ 代表企业或 MSSP。

可能面临黑客攻击的风险，还可能面临由 MSSP 引起的信息泄露风险。我们用 α 表示信息泄漏的概率，泄漏损失为 $\alpha\omega L_{NC}$ 或 $\alpha\omega dL_{NC}$，其中 ω 表示信息泄漏造成的损失与黑客攻击造成的损失之比。需要注意的是，在实践中，当安全服务失败不是由客户端故障引起时，许多 MSSP 会补偿企业，例如 Verizon[2]、BT[3] 和 CenturyLink[4]。因此，我们假设当企业遭受黑客或信息泄漏风险造成的安全损失时，MSSP 会对企业进行补偿，而这些都是 MSSP 侧的失误，也就是说，在信息泄露后，MSSP 还需要按照合同规定的补偿比例(f_i,φ_i)对企业进行补偿。

3.1. OC 策略

我们首先讨论企业采取 OC 策略时的情景。此时核心业务和非核心业务被攻击的概率可以分别表示为 $p_C=1-q_C^m-\beta^{f2m}q_{NC}^f$ 和 $p_{NC}=1-q_{NC}^f-\beta^{m2f}q_C^m$。企业的预期成本包括服务费用、核心和非核心业务的预期安全损失、核心业务信息泄漏造成的损失、MSSP 的预期赔偿以及企业对非核心业务的安全努力成本。因此，企业的预期成本可以描述为：

我们可以获得 OC 策略下企业的预期成本，如下所示：

$$\begin{aligned}W_{OC}=&\ p_Cp_{NC}\left(dL_{NC}\left(1-\varphi_C\right)+L_{NC}\right)+p_C\left(1-p_{NC}\right)dL_{NC}\left(1-\varphi_C\right)+p_{NC}\left(1-p_C\right)L_{NC}\\&+f_C+\frac{1}{2}c_{NC}{q_{NC}^f}^2+\alpha\omega dL_{NC}\left(1-\varphi_C\right)\end{aligned}\tag{1}$$

另一方面，MSSP 的预期收益包括对核心业务施加的安全努力成本、服务费以及核心业务被攻击或核心业务信息被泄露时对企业的预期赔偿。因此，MSSP 的预期收益如下：

$$\pi_{OC}=f_C-p_CdL_{NC}\varphi_C-\frac{1}{2}\eta c_C{q_C^m}^2-\alpha\omega dL_{NC}\varphi_C\tag{2}$$

我们使用 q_C^{m*} 和 ${q_{NC}^f}^*$ 分别代表核心业务的最优安全质量(即 MSSP 对于核心业务的最优安全努力)和非核心业务的最优安全质量(即企业在非核心业务上的最优安全努力)，并确保 MSSP 能够获得保留效用 $\underline{\pi}_M$。通过将攻击概率代入目标函数(1)和(2)并求导，然后用逆向归纳法求解联立方程，我们可以得到最终的均衡解：当企业采用 OC 策略时，企业将赔偿比例设置为 $\varphi_C=\dfrac{\left(\beta^{m2f}+d\right)c_{NC}}{d\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)}$，核心业务的最优安全质量为 $q_C^{m*}=\dfrac{L_{NC}\left(\beta^{m2f}+d\right)c_{NC}}{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)\eta c_C}$，非核心业务的最优安全质量为 ${q_{NC}^f}^*=\dfrac{L_{NC}\left(\left(1-\beta^{f2m}\beta^{m2f}\right)c_{NC}+c_C\eta\beta^{f2m^2}\left(\beta^{f2m}d+1\right)\right)}{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)c_{NC}}$。

证明：当企业采用 OC 策略时，使用反向归纳法，在第二阶段 MSSP 的决策目标是使预期收益最大化，企业的决策目标是使预期成本最小化。MSSP 期望收益和企业预期成本对安全质量的一阶导函数分别为：$\begin{cases}\dfrac{\partial\pi_{OC}}{\partial q_C^m}=dL_{NC}\varphi_C-\eta c_Cq_C^m\\\dfrac{\partial W_{OC}}{\partial q_{NC}^f}=\left(\beta^{f2m}d\left(\varphi_C-1\right)-1\right)L_{NC}+c_{NC}q_{NC}^f\end{cases}$，求解一阶导方程可以得到 MSSP 的最优安全努力为

[2] 详情可见：http://www.verizonenterprise.com/terms/us/products/security/。
[3] 详情可见：https://www2.bt.com/static/i/media/pdf/ip_converge_service_schedule.pdf。
[4] 详情可见：http://www.centurylink.com/legal/docs/Managed-Security-Service.pdf。

$q_C^m=\dfrac{dL_{NC}\varphi_C}{\eta c_C}$，企业的最优安全努力为 $q_{NC}^f=-\dfrac{L_{NC}\left(\beta^{f2m}d\varphi_C-\beta^{f2m}d-1\right)}{c_{NC}}$。

接着建立第一阶段的最优目标函数为：

$$\begin{aligned}M&=-W_{OC}+\lambda\left(\pi_{OC}-\underline{\pi}_M\right)\\&=-p_C p_{NC}\left(dL_{NC}\left(1-\varphi_C\right)+L_{NC}\right)-p_C\left(1-p_{NC}\right)dL_{NC}\left(1-\varphi_C\right)-f_C\\&\quad-p_{NC}\left(1-p_C\right)L_{NC}-\frac{1}{2}c_{NC}{q_{NC}^f}^2-\alpha\omega dL_{NC}\left(1-\varphi_C\right)\\&\quad+\lambda\left(f_C-p_C dL_{NC}\varphi_C-\frac{1}{2}\eta c_C q_C^{m2}-\alpha\omega dL_{NC}\varphi_C-\underline{\pi}_M\right)\end{aligned}$$

，并分别对 φ_C 和 λ 求一阶导得：

$$\begin{cases}\dfrac{\partial M}{\partial\varphi_C}=(1-\lambda)\left(p_C dL_{NC}+\alpha\omega dL_{NC}\right)\\[2ex]\dfrac{\partial M}{\partial\lambda}=f_C-p_C dL_{NC}\varphi_C-\dfrac{1}{2}\eta c_C q_C^{m2}-\alpha\omega dL_{NC}\varphi_C-\underline{\pi}_M\end{cases}$$

。联立求解以上两个一阶导公式可以得到 $\lambda=1$，将 $\lambda=1$、$q_C^m=\dfrac{dL_{NC}\varphi_C}{\eta c_C}$ 和 $q_{NC}^f=-\dfrac{L_{NC}\left(\beta^{f2m}d\varphi_C-\beta^{f2m}d-1\right)}{c_{NC}}$ 带入目标函数 M 中，并对 φ_C 求一阶导并解得 $\varphi_C=\dfrac{\left(\beta^{m2f}+d\right)c_{NC}}{d\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)}$。将 $\varphi_C=\dfrac{\left(\beta^{m2f}+d\right)c_{NC}}{d\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)}$ 代入 $q_C^m=\dfrac{dL_{NC}\varphi_C}{\eta c_C}$ 和 $q_{NC}^f=-\dfrac{L_{NC}\left(\beta^{f2m}d\varphi_C-\beta^{f2m}d-1\right)}{c_{NC}}$，我们可以解得核心业务和非核心业务最优安全质量分别为 $q_C^{m*}=\dfrac{L_{NC}\left(\beta^{m2f}+d\right)c_{NC}}{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)\eta c_C}$ 和 $q_{NC}^{f\ *}=\dfrac{L_{NC}\left(\left(1-\beta^{f2m}\beta^{m2f}\right)c_{NC}+c_C\eta\beta^{f2m^2}\left(\beta^{f2m}d+1\right)\right)}{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)c_{NC}}$。企业的最优预期成本为

$$\begin{aligned}W_{OC}=\frac{1}{2c_C\eta c_{NC}\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)}&\left(\left(2\left(\left(\alpha d\omega+d+1\right)L_{NC}+\underline{\pi}_M\right)c_C\eta-{L_{NC}}^2\left(\beta^{m2f}+d\right)^2\right){c_{NC}}^2\right.\\&\left.-\left(-2\left(\left(\alpha d\omega+d+1\right)L_{NC}+\underline{\pi}_M\right)\beta^{f2m^2}\eta c_C+{L_{NC}}^2\left(\beta^{f2m}d+1\right)^2\right)\eta c_C c_{NC}-{c_C}^2{L_{NC}}^2\eta^2\beta^{f2m^2}\left(\beta^{f2m}d+1\right)^2\right)\end{aligned}$$

。

此时，MSSP 可获得的服务费为

$$\begin{aligned}f_C=\frac{1}{2\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)^2\eta c_C}&\left(2\underline{\pi}_M{c_C}^3\eta^3\beta^{f2m^4}-2\left(\beta^{f2m}\left(\beta^{f2m}d+1\right)\left(\beta^{m2f}+d\right){L_{NC}}^2\right.\right.\\&-c_{NC}\left(\alpha\omega+1\right)\left(\beta^{m2f}+d\right)L_{NC}-2c_{NC}\underline{\pi}_M\Big)\beta^{f2m^2}{c_C}^2\eta^2+2\Big(\beta^{f2m}\left(\beta^{f2m}\beta^{m2f}-1\right)\left(d+\beta^{m2f}\right){L_{NC}}^2\\&\left.\left.+c_{NC}\left(\alpha\omega+1\right)\left(\beta^{m2f}+d\right)L_{NC}+c_{NC}\underline{\pi}_M\Big)c_{NC}c_C\eta-{L_{NC}}^2\left(d+\beta^{m2f}\right)^2{c_{NC}}^2\right)\right.\end{aligned}$$

。

证毕。

从以上均衡解可以发现，在 OC 策略下，企业不能从 MSSP 中获得全部的补偿。此外，由于安全外部性的存在，核心业务和非核心业务的最优安全质量是不同的，取决于许多其它安全因素。

当企业采取 OC 策略时，若核心业务的安全质量受到政府或行业协会设定的强制性安全标准 q_0 约束时，我们可以得到引理 1。

引理 1：

1) 若 $q_0\le q_C^{m*}$，以上基本模型中的最优均衡解不变；

2) 若 $q_0 > q_C^{m*}$，非核心业务的最优安全质量为 $\overline{q_{NC}^{f*}} = \frac{\left(\beta^{f2m}d+1\right)L_{NC}}{c_{NC}}$，核心业务的最优安全质量为 $\overline{q_C^{m*}} = q_0$，企业设置赔偿比例为 $\overline{\varphi_C} = 0$，服务费为 $\overline{f_C} = \frac{\eta c_C q_0^2}{2} + \underline{\pi}_M$。企业的最优期望成本为：$\overline{W_{OC}} = \frac{\left(\left((2\alpha\omega - 2q_0 + 2)d - 2\beta^{m2f}q_0 + 2\right)L_{NC} + \eta c_C q_0^2 + 2\underline{\pi}_M\right)c_{NC} - \left(\beta^{f2m}d+1\right)^2 {L_{NC}}^2}{2c_{NC}}$。

证明：当企业采用 OC 策略时，若 $q_0 \le q_C^{m*}$，证明过程与基本模型相同。若 $q_0 > q_C^{m*}$，使用反向归纳法，在第二阶段 MSSP 负责的核心业务受到强制性安全标准约束，因此可得到 $\overline{q_C^m} = q_0$；同时，企业预期成本对安全质量的一阶导为：$\frac{\partial W_{OC}}{\partial q_{NC}^f} = \left(\beta^{f2m}\left(\varphi_C - 1\right)d - 1\right)L_{NC} + c_{NC}q_{NC}^f$，求解一阶导方程可以得到企业的最优安全质量为 $q_{NC}^f = -\frac{L_{NC}\left(\beta^{f2m}d\varphi_C - \beta^{f2m}d - 1\right)}{c_{NC}}$。

接着建立第一阶段的最优目标函数为：

$$\begin{aligned} M &= -W_{OC} + \lambda\left(\pi_{OC} - \underline{\pi}_M\right) \\ &= -p_C p_{NC}\left(dL_{NC}\left(1-\varphi_C\right) + L_{NC}\right) - p_C\left(1-p_{NC}\right)dL_{NC}\left(1-\varphi_C\right) \\ &\quad - f_C - p_{NC}\left(1-p_C\right)L_{NC} - \frac{1}{2}c_{NC}{q_{NC}^f}^2 - \alpha\omega dL_{NC}\left(1-\varphi_C\right) \\ &\quad + \lambda\left(f_C - p_C dL_{NC}\varphi_C - \frac{1}{2}\eta c_C q_C^{m2} - \alpha\omega dL_{NC}\varphi_C - \underline{\pi}_M\right) \end{aligned},$$

并分别对 φ_C 和 λ 求一阶导得：$\begin{cases} \frac{\partial M}{\partial \varphi_C} = (1-\lambda)\left(p_C dL_{NC} + \alpha\omega dL_{NC}\right) \\ \frac{\partial M}{\partial \lambda} = f_C - p_C dL_{NC}\varphi_C - \frac{1}{2}\eta c_C q_C^{m2} - \alpha\omega dL_{NC}\varphi_C - \underline{\pi}_M \end{cases}$。联立求解以上两个一阶导公式可以得到 $\lambda = 1$，将 $\lambda = 1$、$q_C^m = q_0$ 和 $q_{NC}^f = -\frac{L_{NC}\left(\beta^{f2m}d\varphi_C - \beta^{f2m}d - 1\right)}{c_{NC}}$ 代入目标函数 M 中，并对 φ_C 求一阶导并解得 $\varphi_C = 0$。将 $\varphi_C = 0$ 代入 $q_{NC}^f = -\frac{L_{NC}\left(\beta^{f2m}d\varphi_C - \beta^{f2m}d - 1\right)}{c_{NC}}$，我们可以解得最优安全质量为 $\overline{q_C^{m*}} = q_0$ 和 $\overline{q_{NC}^{f*}} = \frac{L_{NC}\left(\beta^{f2m}d+1\right)}{c_{NC}}$。企业的最优预期成本为 $\overline{W_{OC}} = \frac{\left(\left((2\alpha\omega - 2q_0 + 2)d - 2\beta^{m2f}q_0 + 2\right)L_{NC} + \eta c_C q_0^2 + 2\underline{\pi}_M\right)c_{NC} - \left(\beta^{f2m}d+1\right)^2 {L_{NC}}^2}{2c_{NC}}$，一旦被攻击需付出的赔偿比例为 $\overline{\varphi_C} = 0$。

证毕。

从引理 1 可以发现，当强制性安全标准较高时，企业无需设置赔偿比例即可达到最优决策。

3.2. ONC 策略

我们接下来讨论企业采取 ONC 策略时的情景。在这种情况下，核心业务和非核心业务被攻击的概率可以分别表示为 $p_C = 1 - q_C^f - \beta^{m2f}q_{NC}^m$ 和 $p_{NC} = 1 - q_{NC}^m - \beta^{f2m}q_C^f$。企业的预期成本包括服务费用、核心和非核心业务的预期安全损失、非核心业务信息泄漏造成的损失、MSSP 的预期赔偿以及企业对核心业务的安全努力成本。因此，企业的预期成本可以描述为：

$$W_{ONC} = p_C p_{NC}\left(L_{NC}\left(1-\varphi_{NC}\right)+dL_{NC}\right)+p_{NC}\left(1-p_C\right)L_{NC}\left(1-\varphi_{NC}\right)+p_C\left(1-p_{NC}\right)dL_{NC} + f_{NC}+\frac{1}{2}c_C q_C^{f\,2}+\alpha\omega L_{NC}\left(1-\varphi_{NC}\right) \tag{3}$$

另一方面，根据 ONC 策略，MSSP 的预期收益如下：

$$\pi_{ONC} = f_{NC} - p_{NC}L_{NC}\varphi_{NC} - \frac{1}{2}\eta c_{NC} q_{NC}^{m\,2} - \alpha\omega L_{NC}\varphi_{NC} \tag{4}$$

我们使用 q_C^{f*} 和 $q_{NC}^{m\,*}$ 分别代表核心业务的最优安全质量(即企业对于核心业务的最优安全努力)和非核心业务的最优安全质量(即 MSSP 在非核心业务上的最佳安全努力)，并确保 MSSP 能够获得保留效用 $\underline{\pi}_M$。通过将攻击概率代入目标函数(3)和(4)并求导，然后用逆向归纳法求解联立方程，我们可以得到最终的均衡解：当企业采用 ONC 策略时，企业将赔偿比例设置为 $\varphi_{NC} = \dfrac{\left(d\beta^{m2f}+1\right)c_C}{c_{NC}\eta\beta^{f2m^2}+c_C}$。核心业务的最优安全质量为 $q_C^{f*} = -\dfrac{\left(d\left(\beta^{f2m}\beta^{m2f}-1\right)c_C - c_{NC}\eta\beta^{f2m^2}\left(d+\beta^{f2m}\right)\right)L_{NC}}{\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)c_C}$，非核心业务的最优安全质量为 $q_{NC}^{m\,*} = \dfrac{L_{NC}\left(d\beta^{m2f}+1\right)c_C}{\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)\eta c_{NC}}$。

证明：证明过程可参考 3.1 节基本模型，在此不过多赘述。

证毕。

当企业采取 ONC 策略时，若核心业务的安全质量受到政府或行业协会设定的强制性安全标准 q_0 约束时，我们可以得到引理 2。

引理 2：

1) 若 $q_0 \le q_C^{f*}$，以上基本模型中的最优解不变；

2) 若 $q_0 > q_C^{f*}$，非核心业务的最优安全质量为 $\overline{q_{NC}^{m}}^{*} = \dfrac{L_{NC}\left(d\beta^{m2f}+1\right)}{\eta c_{NC}}$，核心业务的最优安全质量为 $\overline{q_C^{f}}^{*} = q_0$，企业设置赔偿比例为 $\overline{\varphi_{NC}} = \beta^{m2f}d+1$，服务费为 $\overline{f_{NC}} = \dfrac{-L_{NC}^{\,2}\left(d\beta^{m2f}+1\right)^2 - 2\eta c_{NC}\left(-\alpha\omega+q_0\beta^{f2m}-1\right)\left(d\beta^{m2f}+1\right)L_{NC}+2\underline{\pi}_M\eta c_{NC}}{2\eta c_{NC}}$。企业的最优期望成本为 $\overline{W_{ONC}} = \dfrac{-\left(2\left(\left(q_0-1\right)d+q_0\beta^{f2m}-\alpha\omega-1\right)L_{NC}-c_C q_0^2-2\underline{\pi}_M\right)\eta c_{NC}-L_{NC}^{\,2}\left(d\beta^{m2f}+1\right)^2}{2\eta c_{NC}}$。

证明：证明过程可参考引理 1，在此不过多赘述。

此外，为了确保决策变量 $q_i^j \in (0,1)$，我们得到必要条件

$$L_{NC} < \min\left\{\frac{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)\eta c_C}{\left(\beta^{m2f}+d\right)c_{NC}}, \frac{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)c_{NC}}{\left(1-\beta^{f2m}\beta^{m2f}\right)c_{NC}+c_C\eta\beta^{f2m^2}\left(\beta^{f2m}d+1\right)}, \frac{\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)\eta c_{NC}}{\left(d\beta^{m2f}+1\right)c_C}, -\frac{\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)c_C}{d\left(\beta^{f2m}\beta^{m2f}-1\right)c_C-c_{NC}\eta\beta^{f2m^2}\left(d+\beta^{f2m}\right)}, \frac{\eta c_{NC}}{d\beta^{m2f}+1}\right\}$$

永远成立，此条件确保我们在 OC 和 ONC 两种安全策略中可以解得符合实践的最优解。

证毕。

引理 2 可以发现，在强制性安全需求 q_0 约束下采取 ONC 策略时，不同于 OC 策略下，企业仍需通过规定赔偿比例来确保 MSSP 付出的安全努力。

4. 均衡分析

4.1. 不同安全标准下最优策略比较

接着我们对不同水平安全标准下的最优决策进行比较，探究较为严格的安全标准对企业和 MSSP 最优投资决策行为的影响。

命题 1：

1) 当企业采取 OC 策略时，若 MSSP 负责的核心业务的安全质量受到较高的强制性安全标准约束(即 $q_0 > q_C^{m*}$ 时)，MSSP 赔偿比例变小，即 $\overline{\varphi_C} < \varphi_C$；而企业负责的非核心业务的安全质量在 f2m 外部性为正时变大，在 f2m 外部性为负时变小，即 $\begin{cases} \overline{q_{NC}^f} < q_{NC}^f, & -1 < \beta^{f2m} < 0 \\ \overline{q_{NC}^f} > q_{NC}^f, & 0 < \beta^{f2m} < 1 \end{cases}$。

2) 当企业采取 ONC 策略时，若企业负责的核心业务的安全质量受到较高强制性安全标准约束时(即 $q_0 > q_C^{f*}$ 时)，MSSP 的赔偿比例变大，即 $\overline{\varphi_{NC}} > \varphi_{NC}$；MSSP 提供的非核心业务的安全质量也变大，即 $\overline{q_{NC}^m} > q_{NC}^m$。

证明：企业采取 OC 策略时，对 MSSP 赔偿比例及非核心业务的安全质量受到安全标准约束前后的解作差得 $\overline{\varphi_C} - \varphi_C = 0 - \dfrac{\left(\beta^{m2f} + d\right)c_{NC}}{d\left(c_C\eta\beta^{f2m^2} + c_{NC}\right)} = -\dfrac{\left(\beta^{m2f} + d\right)c_{NC}}{d\left(c_C\eta\beta^{f2m^2} + c_{NC}\right)} < 0$ 且

$\overline{q_{NC}^f} - q_{NC}^f = \dfrac{\left(\beta^{f2m}d + 1\right)L_{NC}}{c_{NC}} - \dfrac{L_{NC}\left(\left(1 - \beta^{f2m}\beta^{m2f}\right)c_{NC} + c_C\eta\beta^{f2m^2}\left(\beta^{f2m}d + 1\right)\right)}{\left(c_C\eta\beta^{f2m^2} + c_{NC}\right)c_{NC}} = \dfrac{L_{NC}\beta^{f2m}\left(\beta^{m2f} + d\right)}{c_C\eta\beta^{f2m^2} + c_{NC}}$，从而得到 $\begin{cases} \overline{q_{NC}^f} < q_{NC}^f, & -1 < \beta^{f2m} < 0 \\ \overline{q_{NC}^f} > q_{NC}^f, & 0 < \beta^{f2m} < 1 \end{cases}$。而企业采取 ONC 策略时，对 MSSP 赔偿比例及非核心业务的安全质量受到安全标准约束前后的解作差得 $\overline{\varphi_{NC}} - \varphi_{NC} = \beta^{m2f}d + 1 - \dfrac{\left(d\beta^{m2f} + 1\right)c_C}{c_{NC}\eta\beta^{f2m^2} + c_C} = \dfrac{c_{NC}\eta\beta^{f2m^2}\left(d\beta^{m2f} + 1\right)}{c_{NC}\eta\beta^{f2m^2} + c_C} > 0$ 且

$\overline{q_{NC}^m} - q_{NC}^m = \dfrac{L_{NC}\left(d\beta^{m2f} + 1\right)}{\eta c_{NC}} - \dfrac{L_{NC}\left(d\beta^{m2f} + 1\right)c_C}{\left(c_{NC}\eta\beta^{f2m^2} + c_C\right)\eta c_{NC}} = \dfrac{L_{NC}\left(d\beta^{m2f} + 1\right)\beta^{f2m^2}}{c_{NC}\eta\beta^{f2m^2} + c_C} > 0$。

证毕。

从命题 1 可以看出：当企业采取 ONC 策略时，若核心业务的安全质量受到较高的强制性安全标准约束，即使此时非核心业务的安全质量并没有受到约束，其安全质量也会相应提高；然而，当企业选择 OC 策略时，若核心业务的安全质量受到较高的强制性安全标准约束，非核心业务安全质量有可能会下降。此外，当企业选择 OC 策略时，核心业务安全质量受到较高的强制性安全标准约束后赔偿比例会降低，因为企业无需再通过规定赔偿比例来确保 MSSP 付出的安全努力；反之，当企业选择 ONC 策略时，核心业务安全质量受到强制性安全标准约束后 MSSP 赔偿比例会升高，因为企业需要规定更高的赔偿比例来确保非核心业务的安全质量。

4.2. 安全外部性的影响

首先我们分析当企业采取 OC 策略时，安全外部性对企业和 MSSP 最优决策的影响。

命题 2：

当企业采用 OC 策略时，若 MSSP 负责的核心业务的安全质量受到较低的强制性安全标准约束时(即 $q_0 \le q_C^{m*}$ 时)核心业务的安全质量随着 f2m 外部性的增加而先增后减，即 $\begin{cases} \dfrac{\partial q_C^m}{\partial \beta^{f2m}} > 0, & -1 < \beta^{f2m} < 0 \\ \dfrac{\partial q_C^m}{\partial \beta^{f2m}} < 0, & 0 < \beta^{f2m} < 1 \end{cases}$；然而非核心业务的安全质量在负 f2m 外部性下随着 m2f 外部性增大而一直增大，而在正 f2m 外部性下随着 m2f 外部性增大而一直减小，即 $\begin{cases} \dfrac{\partial q_{NC}^f}{\partial \beta^{m2f}} > 0, \text{其中 } -1 < \beta^{f2m} < 0 \\ \dfrac{\partial q_{NC}^f}{\partial \beta^{m2f}} < 0, \text{其中 } 0 < \beta^{f2m} < 1 \end{cases}$。

证明：企业采取 OC 策略时，核心业务最优安全质量对 β^{f2m} 的一阶导为 $\dfrac{\partial q_C^m}{\partial \beta^{f2m}} = -\dfrac{2L_{NC}\left(\beta^{m2f}+d\right)\beta^{f2m}c_{NC}}{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)^2}$，非核心业务最优安全质量对 β^{m2f} 的一阶导为 $\dfrac{\partial q_{NC}^f}{\partial \beta^{m2f}} = -\dfrac{L_{NC}\beta^{f2m}}{c_C\eta\beta^{f2m^2}+c_{NC}}$。通过解 $\dfrac{\partial q_C^m}{\partial \beta^{f2m}} = 0$，我们可以得到 $\beta^{f2m}{}_0 = 0$。结果可得到，当 $-1 < \beta^{f2m} < 0$ 时，$\dfrac{\partial q_C^m}{\partial \beta^{f2m}} > 0$；当 $0 < \beta^{f2m} < 1$ 时，$\dfrac{\partial q_C^m}{\partial \beta^{f2m}} < 0$。同时，当 $-1 < \beta^{f2m} < 0$ 时，$\dfrac{\partial q_{NC}^f}{\partial \beta^{m2f}} > 0$；当 $0 < \beta^{f2m} < 1$ 时，$\dfrac{\partial q_{NC}^f}{\partial \beta^{m2f}} < 0$。

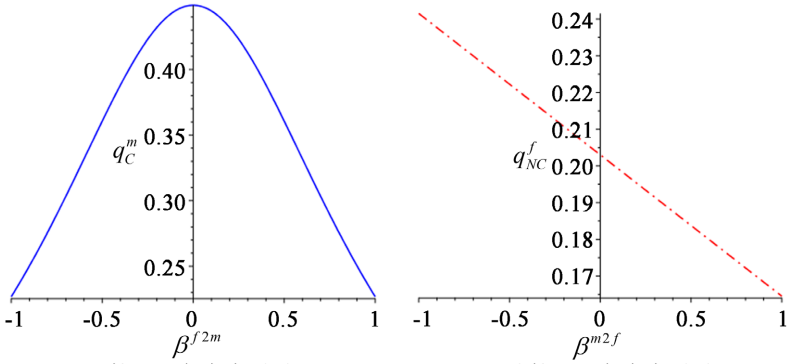
证毕。

需要注意的是，我们主要关注一方的外部性如何影响另一方的决策，也就是说，我们讨论了 f2m (m2f) 外部性对 MSSP(企业)决策的影响，因为决策者更关心另一方如何影响自己的决策，而不是自己如何影响对方的决策。我们发现，当企业采用 OC 策略时，在 m2f 外部性不断增大的情况下，非核心业务的安全质量在负 f2m 外部性下总是增大，在正 f2m 外部条件下总是减小，原因如下。对于企业而言，如果其对 MSSP 的外部性(即 f2m 外部性)为正，则 MSSP 有动机减少安全努力以节约成本，因为核心业务的攻击概率 $p_C = 1 - q_C^m - \beta^{f2m} q_{NC}^f$ 由 MSSP 负责。然而，随着 m2f 外部性的增强，负责非核心业务违约概率 $p_{NC} = 1 - q_{NC}^f - \beta^{m2f} q_C^m$ 的企业希望 MSSP 能够改进其安全工作，因为它可以降低 p_{NC}。因此，当 f2m 外部性为正时，企业会减少其努力，以促使 MSSP 增加努力，从而享受到 m2f 外部性增强的好处，f2m 外部性为负时的原因与为正时的原因相似。因此，企业和 MSSP 双方评估安全外部性的值并做出适当的安全努力至关重要。

我们可以通过设置参数 $L_{NC} = 5, c_C = 35, c_{NC} = 25, \eta = 0.7, d = 2, \beta^{m2f} = 0.2, \beta^{f2m} = 0.2$ 得到命题 2 的结果，如图 1 所示。

命题 3：

当企业采用 OC 策略时，若 MSSP 负责的核心业务的安全质量受到较高强制性安全标准约束时(即 $q_0 > q_C^{m*}$ 时)，非核心业务安全质量不受 m2f 外部性的影响，即 $\dfrac{\partial \overline{q_{NC}^f}}{\partial \beta^{m2f}} = 0$。



(a) 核心业务安全质量　　(b) 非核心业务安全质量

Figure 1. Security quality with security externality under OC strategy
图 1. OC 策略下安全质量随安全外部性的变化

证明：证明过程较直观，在此省略不写。

证毕。

从命题 3 可看出，由于此时核心业务的安全质量为定值，故企业负责的非核心业务的安全质量不受 m2f 外部性的影响。

接着我们讨论当企业采取 ONC 策略时，安全外部性对企业和 MSSP 最优决策的影响。

命题 4：

当企业采用 ONC 策略时，若企业负责的核心业务的安全质量受到较低的强制性安全标准约束时(即 $q_0 \le q_C^{f*}$ 时)非核心业务的安全质量随着 f2m 外部性的增加而先增后减，即 $\begin{cases} \dfrac{\partial q_{NC}^m}{\partial \beta^{f2m}} > 0,\ -1 < \beta^{f2m} < 0 \\ \dfrac{\partial q_{NC}^m}{\partial \beta^{f2m}} < 0,\ 0 < \beta^{f2m} < 1 \end{cases}$；然而核心业务的安全质量在负 f2m 外部性下随着 m2f 外部性的增大而增大，在正 f2m 外部下随着 m2f 的外部性的增大而减小，即 $\begin{cases} \dfrac{\partial q_C^f}{\partial \beta^{m2f}} > 0,\ \text{其中}\ -1 < \beta^{f2m} < 0 \\ \dfrac{\partial q_C^f}{\partial \beta^{m2f}} < 0,\ \text{其中}\ 0 < \beta^{f2m} < 1 \end{cases}$。

证明：企业采取 ONC 策略时，非核心业务安全质量对 β^{f2m} 的一阶导函数为 $\dfrac{\partial q_{NC}^m}{\partial \beta^{f2m}} = -\dfrac{2L_{NC}\left(d\beta^{m2f}+1\right)\beta^{f2m}c_C}{\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)^2}$，核心业务安全质量对 β^{m2f} 的一阶导函数为 $\dfrac{\partial q_C^f}{\partial \beta^{m2f}} = -\dfrac{L_{NC}d\beta^{f2m}}{c_{NC}\eta\beta^{f2m^2}+c_C}$。

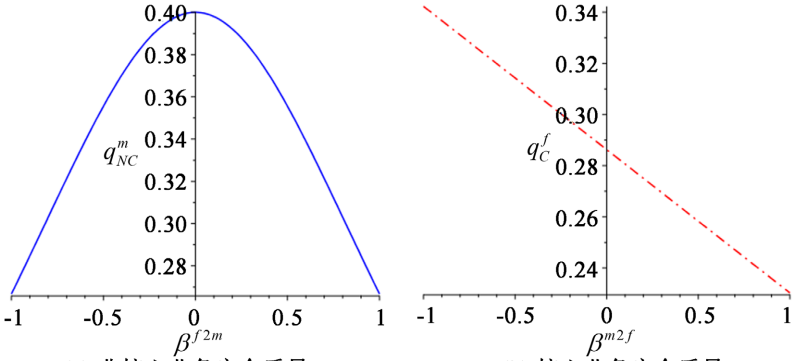
通过解 $\dfrac{\partial q_{NC}^m}{\partial \beta^{f2m}} = 0$，我们可以得到 $\beta^{f2m}{}_1 = 0$，从而得到当 $-1 < \beta^{f2m} < 0$ 时，$\dfrac{\partial q_{NC}^m}{\partial \beta^{f2m}} > 0$；当 $0 < \beta^{f2m} < 1$ 时，$\dfrac{\partial q_{NC}^m}{\partial \beta^{f2m}} < 0$。同时可得到，当 $-1 < \beta^{f2m} < 0$ 时，$\dfrac{\partial q_C^f}{\partial \beta^{m2f}} > 0$；当 $0 < \beta^{f2m} < 1$ 时，$\dfrac{\partial q_C^f}{\partial \beta^{m2f}} < 0$。

证毕。

与前面的命题类似，我们关注一方的外部性如何影响另一方的决策，也就是说，我们讨论了 f2m (m2f) 外部性对 MSSP(企业)决策的影响。我们发现，当企业采取 ONC 策略时，在 m2f 外部性增强的情况下，核心业务的安全质量在负 f2m 外部性下总是增大，在正 f2m 外部条件下总是减小。原因如下。对于企业而言，如果其对 MSSP 的外部性(即 f2m 外部性)为正，则 MSSP 有动机减少安全努力以节省成本，因为

非核心业务的攻击概率为 $p_{NC}=1-q_{NC}^{m}-\beta^{f2m}q_{C}^{f}$。然而，随着 m2f 外部性的增强，负责核心业务攻击概率 $p_{C}=1-q_{C}^{f}-\beta^{m2f}q_{NC}^{m}$ 的企业希望 MSSP 能够提高其安全努力，因为它可以降低 p_{C}。因此，当 f2m 外部性为正时，企业会减少安全努力，以促使 MSSP 增加努力，从而享受到增大的 m2f 外部性的好处，这与命题 1 类似，当 f2m 外部性为负时的原因与为正时的原因也类似。

我们可以通过设置参数 $L_{NC}=5, c_{C}=35, c_{NC}=25, \eta=0.7, d=2, \beta^{m2f}=0.2, \beta^{f2m}=0.2$ 得到命题 4 的结果，如图 2 所示。



(a) 非核心业务安全质量　　(b) 核心业务安全质量

Figure 2. Security quality with security externality under ONC strategy
图 2. ONC 策略下安全质量随安全外部性的变化

命题 5：

当企业采用 ONC 策略时，若企业负责的核心业务的安全质量受到较高强制性安全标准约束时(即 $q_{0}>q_{C}^{f*}$ 时)，非核心业务安全质量不受 f2m 外部性的影响，即 $\frac{\partial\overline{q_{NC}^{m}}}{\partial\beta^{f2m}}=0$。

证明：证明过程较直观，在此省略不写。

证毕。

从命题 5 可以看出，当强制性安全标准水平较高时，由于此时核心业务的安全质量为一个定值，即等于安全标准，非核心业务的安全质量不受另一方决策主体安全外部性的影响，此结论与命题 3 类似。

4.3. 企业策略选择

最后我们研究在不同范围的强制性安全标准约束下企业如何针对部分外包策略(OC 和 ONC 策略)做出选择。

当 $q_{0}<\min\left\{q_{C}^{m*}, q_{C}^{f*}\right\}$ 时，企业采取核心或非核心外包策略时的最优决策如表 3 所示，代入企业预期成本函数可得企业采取 OC 和 ONC 策略下的成本分别为：

$$W_{OC}=\frac{1}{2c_{C}\eta c_{NC}\left(c_{C}\eta\beta^{f2m^{2}}+c_{NC}\right)}\left(\left(2\left((\alpha d\omega+d+1)L_{NC}+\underline{\pi}_{M}\right)c_{C}\eta-L_{NC}^{2}\left(\beta^{m2f}+d\right)^{2}\right)c_{NC}^{2}\right.$$

和

$$\left.-\left(-2\left((\alpha d\omega+d+1)L_{NC}+\underline{\pi}_{M}\right)\beta^{f2m^{2}}\eta c_{C}+L_{NC}^{2}\left(\beta^{f2m}d+1\right)^{2}\right)\eta c_{C}c_{NC}-c_{C}^{2}L_{NC}^{2}\eta^{2}\beta^{f2m^{2}}\left(1+\beta^{f2m}d\right)^{2}\right)$$

$$W_{ONC}=\frac{1}{2c_{C}\eta c_{NC}\left(c_{NC}\eta\beta^{f2m^{2}}+c_{C}\right)}\left(-\eta^{2}\beta^{f2m^{2}}\left(\left(-2\alpha\omega-2d-2\right)L_{NC}-2\underline{\pi}_{M}\right)c_{C}L_{NC}^{2}\left(\beta^{f2m}+d\right)^{2}\right)c_{NC}^{2}$$

，我们可

$$\left.-\eta c_{C}\left(\left(\left(-2\alpha\omega-2d-2\right)L_{NC}-2\underline{\pi}_{M}\right)c_{C}+L_{NC}^{2}\left(\beta^{f2m}+d\right)^{2}\right)c_{NC}-c_{C}^{2}L_{NC}^{2}\left(\beta^{m2f}d+1\right)^{2}\right)$$

据此可以得到命题 6。

Table 3. Equilibrium results under lower security standards
表 3. 安全标准较低时的最优安全决策

策略	$\overline{q_i^j}$	
OC 策略	$q_{NC}^f = \frac{L_{NC}\left(\left(1-\beta^{f2m}\beta^{m2f}\right)c_{NC}+c_C\eta\beta^{f2m^2}\left(\beta^{f2m}d+1\right)\right)}{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)c_{NC}}$	$q_C^m = \frac{L_{NC}\left(\beta^{m2f}+d\right)c_{NC}}{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)\eta c_C}$
ONC 策略	$q_C^f = -\frac{\left(d\left(\beta^{f2m}\beta^{m2f}-1\right)c_C-c_{NC}\eta\beta^{f2m^2}\left(d+\beta^{f2m}\right)\right)L_{NC}}{\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)c_C}$	$q_{NC}^m = \frac{L_{NC}\left(d\beta^{m2f}+1\right)c_C}{\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)\eta c_{NC}}$

命题 6：当强制性安全标准较低($q_0 < \min\left\{q_C^{m*}, q_C^{f*}\right\}$)时，若信息泄露的可能性较低，企业将采取 OC 策略，若信息泄露的可能性较高，企业将采取 ONC 策略，即 $\begin{cases} W_{ONC} > W_{OC}, & \alpha < \alpha_1 \\ W_{ONC} \le W_{OC}, & \alpha \ge \alpha_1 \end{cases}$，其中

$$\alpha_1 = \frac{1}{2c_C\eta c_{NC}\left(\beta^{f2m^2}c_C\eta+c_{NC}\right)\left(\beta^{f2m^2}c_{NC}\eta+c_C\right)\omega(d-1)}\left(\left(-\beta^{f2m^2}\eta\left(\left(\beta^{f2m}+d\right)^2\eta-\left(\beta^{m2f}+d\right)^2\right)c_{NC}{}^3\right.\right.$$
$$-c_C\left(\beta^{f2m^4}\left(d+\beta^{f2m}\right)^2\eta^3-\beta^{f2m^2}\left(d\beta^{f2m}+1\right)^2\eta^2+\left(\beta^{f2m}+d\right)^2\eta-\left(\beta^{m2f}+d\right)^2\right)c_{NC}{}^2$$
$$+\left(\beta^{f2m^4}\left(d\beta^{f2m}+1\right)^2\eta^3-\beta^{f2m^2}\left(\beta^{f2m}+d\right)^2\eta^2+\left(d\beta^{f2m}+1\right)^2\eta-\left(d\beta^{f2m}+1\right)^2\right)c_C{}^2c_{NC}$$
$$\left.\left.+\beta^{f2m^2}\eta c_C{}^3\left(\left(d\beta^{f2m}+1\right)^2\eta-\left(d\beta^{m2f}+1\right)^2\right)\right)L_{NC}\right)$$

。

证明：通过解 $W_{ONC}-W_{OC}=0$，我们可以得到

$$\alpha_1 = \frac{1}{2c_C\eta c_{NC}\left(\beta^{f2m^2}c_C\eta+c_{NC}\right)\left(\beta^{f2m^2}c_{NC}\eta+c_C\right)\omega(d-1)}\left(\left(-\beta^{f2m^2}\eta\left(\left(\beta^{f2m}+d\right)^2\eta-\left(\beta^{m2f}+d\right)^2\right)c_{NC}{}^3\right.\right.$$
$$-c_C\left(\beta^{f2m^4}\left(d+\beta^{f2m}\right)^2\eta^3-\beta^{f2m^2}\left(d\beta^{f2m}+1\right)^2\eta^2+\left(\beta^{f2m}+d\right)^2\eta-\left(\beta^{m2f}+d\right)^2\right)c_{NC}{}^2$$
$$+\left(\beta^{f2m^4}\left(d\beta^{f2m}+1\right)^2\eta^3-\beta^{f2m^2}\left(\beta^{f2m}+d\right)^2\eta^2+\left(d\beta^{f2m}+1\right)^2\eta-\left(d\beta^{f2m}+1\right)^2\right)c_C{}^2c_{NC}$$
$$\left.\left.+\beta^{f2m^2}\eta c_C{}^3\left(\left(d\beta^{f2m}+1\right)^2\eta-\left(d\beta^{m2f}+1\right)^2\right)\right)L_{NC}\right)$$

。因为

$\frac{\partial\left(W_{ONC}-W_{OC}\right)}{\partial\alpha} = (1-d)\omega L_{NC} < 0$，我们可以得出当 $\alpha < \alpha_1$ 时，$W_{ONC} > W_{OC}$；当 $\alpha \ge \alpha_1$ 时，$W_{ONC} \le W_{OC}$。

证毕。

若强制性安全标准位于中等水平($q_C^{m*} < q_0 < q_C^{f*}$)时，企业采取 OC 策略时企业和 MSSP 双方的最优安全决策受到强制性安全标准的影响，采取 ONC 策略时企业和 MSSP 的最优决策不受安全标准限制。此时企业在 OC 策略和 ONC 策略下的最优决策如表 4 所示。企业在两种策略下的成本分别为：

$\overline{W_{OC}} = \frac{\left(\left((2\alpha\omega-2q_0+2)d-2\beta^{m2f}q_0+2\right)L_{NC}+\eta c_C q_0^2+2\underline{\pi}_M\right)c_{NC}-\left(\beta^{f2m}d+1\right)^2L_{NC}{}^2}{2c_{NC}}$ 和

$$W_{ONC} = \frac{1}{2c_C\eta c_{NC}\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)}\left(-\eta^2\beta^{f2m^2}\left(\left((-2\alpha\omega-2d-2)L_{NC}-2\underline{\pi}_M\right)c_CL_{NC}{}^2\left(\beta^{f2m}+d\right)^2\right)c_{NC}{}^2\right.$$
$$\left.-\eta c_C\left(\left((-2\alpha\omega-2d-2)L_{NC}-2\underline{\pi}_M\right)c_C+L_{NC}{}^2\left(\beta^{f2m}+d\right)^2\right)c_{NC}-c_C{}^2L_{NC}{}^2\left(\beta^{m2f}d+1\right)^2\right)$$

，因此可

以得到命题 7。

Table 4. Equilibrium results under first medium security standards
表 4. 安全标准位于第一种中等水平时的最优安全决策

策略	q_i^j	
OC 策略	$q_{NC}^f = \frac{\left(\beta^{f2m}d+1\right)L_{NC}}{c_{NC}}$	$q_C^m = q_0$
ONC 策略	$q_C^f = -\frac{\left(d\left(\beta^{f2m}\beta^{m2f}-1\right)c_C - c_{NC}\eta\beta^{f2m^2}\left(d+\beta^{f2m}\right)\right)L_{NC}}{\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)c_C}$	$q_{NC}^m = \frac{L_{NC}\left(d\beta^{m2f}+1\right)c_C}{\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)\eta c_{NC}}$

命题 7：当强制性安全标准位于中等水平($q_C^{m*} < q_0 < q_C^{f*}$)时，若信息泄露的可能性较低，企业将采取 OC 策略，若信息泄露的可能性较高，企业将采取 ONC 策略，即 $\begin{cases}\overline{W_{ONC}} > W_{OC}, & \alpha < \alpha_2 \\ \overline{W_{ONC}} \le W_{OC}, & \alpha \ge \alpha_2\end{cases}$，其中

$$\alpha_2 = \frac{1}{2L_{NC}\omega(d-1)c_C\eta c_{NC}\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)}\left(\left(c_{NC}\beta^{f2m^2}\left(\left(d\beta^{f2m}+1\right)^2c_C - c_{NC}\left(d+\beta^{f2m}\right)^2\right)\eta^2\right.\right.$$
$$+c_C\left(\left(d\beta^{f2m}+1\right)^2c_C - c_{NC}\left(d+\beta^{f2m}\right)^2\right)\eta - {c_C}^2\left(d\beta^{m2f}+1\right)^2\Big){L_{NC}}^2$$
$$\left.+2c_Cc_{NC}\eta q_0\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)\left(\beta^{m2f}+d\right)L_{NC} - {c_C}^2c_{NC}\eta^2{q_0}^2\left(c_{NC}\eta\beta^{f2m^2}+c_C\right)\right)$$

。

证明：证明过程可参考命题 6，在此不过多赘述。

证毕。

若强制性安全标准位于中等水平($q_C^{f*} < q_0 < q_C^{m*}$)时，企业采取 OC 策略时企业和 MSSP 的最优决策不受安全标准约束，采取 ONC 策略时企业和 MSSP 双方的最优安全决策受到强制性安全标准的影响，此时企业在 OC 策略和 ONC 策略下的最优决策如表 5 所示，采取核心外包和非核心外包策略下的成本分别为：

$$W_{OC} = \frac{1}{2c_C\eta c_{NC}\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)}\left(\left(2\left(\left(\alpha d\omega+d+1\right)L_{NC}+\underline{\pi}_M\right)c_C\eta - {L_{NC}}^2\left(\beta^{m2f}+d\right)^2\right){c_{NC}}^2\right.$$
$$\left.-\left(-2\left(\left(\alpha d\omega+d+1\right)L_{NC}+\underline{\pi}_M\right)\beta^{f2m^2}\eta c_C + {L_{NC}}^2\left(\beta^{f2m}d+1\right)^2\right)\eta c_Cc_{NC} - {c_C}^2{L_{NC}}^2\eta^2\beta^{f2m^2}\left(1+\beta^{f2m}d\right)^2\right)$$

和 $\overline{W_{ONC}} = \frac{-\left(2\left(\left(q_0-1\right)d+q_0\beta^{f2m}-\alpha\omega-1\right)L_{NC} - c_Cq_0^2 - 2\underline{\pi}_M\right)\eta c_{NC} - {L_{NC}}^2\left(d\beta^{m2f}+1\right)^2}{2\eta c_{NC}}$，因此可以得到命题 8。

Table 5. Equilibrium results under second medium security standards
表 5. 安全标准位于第二种中等水平时的最优安全决策

策略	q_i^j	
OC 策略	$q_{NC}^f = \frac{L_{NC}\left(\left(1-\beta^{f2m}\beta^{m2f}\right)c_{NC}+c_C\eta\beta^{f2m^2}\left(\beta^{f2m}d+1\right)\right)}{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)c_{NC}}$	$q_C^m = \frac{L_{NC}\left(\beta^{m2f}+d\right)c_{NC}}{\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)\eta c_C}$
ONC 策略	$q_C^f = q_0$	$q_{NC}^m = \frac{L_{NC}\left(d\beta^{m2f}+1\right)}{\eta c_{NC}}$

命题 8：当强制性安全标准位于中等水平($q_C^{f*} < q_0 < q_C^{m*}$)时，若信息泄露的可能性较低，企业将采取 OC 策略，若信息泄露的可能性较高，企业将采取 ONC 策略，即 $\begin{cases}\overline{W_{ONC}} > W_{OC}, \alpha < \alpha_3 \\ \overline{W_{ONC}} \le W_{OC}, \alpha \ge \alpha_3\end{cases}$，其中

$$\alpha_3 = \frac{1}{2L_{NC}\omega(d-1)c_C\eta c_{NC}\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)}\left(\left(\eta\left(\left(d\beta^{f2m}+1\right)^2\eta-\left(d\beta^{m2f}+1\right)^2\right)\beta^{f2m^2}c_C{}^2\right.\right.$$
$$+c_{NC}\left(\left(d\beta^{f2m}+1\right)^2\eta-\left(d\beta^{m2f}+1\right)^2\right)c_C+c_{NC}{}^2\left(d+\beta^{m2f}\right)^2\Big)L_{NC}{}^2 \quad 。$$
$$\left.\left.-2c_Cc_{NC}\eta q_0\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)\left(d+\beta^{f2m}\right)L_{NC}+c_C{}^2c_{NC}\eta q_0{}^2\left(c_C\eta\beta^{f2m^2}+c_{NC}\right)\right)\right)$$

证明：证明过程可参考命题 6，在此不过多赘述。

证毕。

当强制性安全标准较高($q_0 > \max\left\{q_C^{m*}, q_C^{f*}\right\}$)时，企业采取 OC 策略和 ONC 策略时企业和 MSSP 双方的最优安全决策均会受到强制性安全标准的影响。此时企业在核心外包和非核心外包策略下的最优决策如表 6 所示。企业采取核心外包和非核心外包策略下的成本分别为：

$\overline{W_{OC}} = \dfrac{\left(\left((2\alpha\omega-2q_0+2)d-2\beta^{m2f}q_0+2\right)L_{NC}+\eta c_Cq_0^2+2\underline{\pi}_M\right)c_{NC}-\left(\beta^{f2m}d+1\right)^2L_{NC}{}^2}{2c_{NC}}$ 和

$\overline{W_{ONC}} = \dfrac{-\left(2\left((q_0-1)d+q_0\beta^{f2m}-\alpha\omega-1\right)L_{NC}-c_Cq_0^2-2\underline{\pi}_M\right)\eta c_{NC}-L_{NC}{}^2\left(d\beta^{m2f}+1\right)^2}{2\eta c_{NC}}$，因此可以得到命题 9。

Table 6. Equilibrium results under higher security standards
表 6. 安全标准较高时的最优安全决策

策略	q_i^j	
OC 策略	$q_{NC}^f = \dfrac{\left(\beta^{f2m}d+1\right)L_{NC}}{c_{NC}}$	$q_C^m = q_0$
ONC 策略	$q_C^f = q_0$	$q_{NC}^m = \dfrac{L_{NC}\left(d\beta^{m2f}+1\right)}{\eta c_{NC}}$

命题 9：当信息泄露的可能性较低时，企业将采取 OC 策略，当信息泄露的可能性较高时，企业将采取 ONC 策略。即 $\begin{cases}\overline{W_{ONC}} > \overline{W_{OC}}, \alpha < \alpha_4 \\ \overline{W_{ONC}} \le \overline{W_{OC}}, \alpha \ge \alpha_4\end{cases}$，其中 $\alpha_4 = \dfrac{1}{2\eta c_{NC}\omega(d-1)L_{NC}}\left(\left(\left(d\beta^{f2m}+1\right)^2\eta-\left(d\beta^{m2f}+1\right)^2\right)L_{NC}{}^2\right.$ $\left.-2\eta c_{NC}\left(\beta^{f2m}-\beta^{m2f}\right)q_0L_{NC}-c_Cc_{NC}\eta q_0{}^2(\eta-1)\right)$ 。

证明：证明过程可参考命题 6，在此不过多赘述。

证毕。

从以上几个命题中可看出无论在多高的强制性安全标准约束下，企业总是在信息泄露风险较高时选择 ONC 策略，在信息泄露风险较低时选择 OC 策略。

5. 结论与展望

复杂的网络安全环境迫使许多企业将其信息业务外包给 MSSP。在实践中，由于信息泄露风险的存在，许多企业选择部分外包策略来抵御黑客的攻击。然而，目前对部分外包策略下的安全外部性的研究

非常有限。因此，在前人研究的基础上，我们采用博弈论模型来考察安全外部性在 MSSP 和企业安全外包激励中的作用，为企业的安全实践提供管理启示。

本文从安全外部性不对称的视角研究了企业和 MSSP 合作保护核心和非核心业务的情景，并考虑了强制性安全标准的影响，补充了关于安全问题的新结论。我们发现，当强制性安全标准较低时，若企业对 MSSP 的外部性为负(正)，企业付出的安全努力水平总是随着 MSSP 对企业外部性的增大而增大(减小)。当强制性安全标准较高时，企业或 MSSP 的最优决策不受另一方外部性的影响。另外，我们发现，当企业采取 OC 策略时，在较低的强制性安全标准约束下，企业需设定一定的赔偿比例从而得到最低期望成本；然而，在较高的强制性安全标准约束下，企业无需设立赔偿机制即可达到最优决策。此外，无论在多高的强制性安全标准约束下，企业总是在信息泄露风险较高时选择 ONC 策略，在信息泄露风险较低时选择 OC 策略。

本文的研究为企业安全外包的策略选择提供了一定的指导依据，但也存在以下局限性：1) 本文从信息安全保护的投资方进行考虑，尚未考虑到黑客行为对企业或者 MSSP 投资行为的影响，未来可以将策略黑客纳入研究范围。2) 企业可能是风险厌恶的，信息安全参与者风险偏好不同的模型值得研究。

参考文献

[1] 瑞星 2021 年中国网络安全报告[R]. 北京: 北京瑞星网安技术股份有限公司, 2022.

[2] Sierra Wireless. 无线设备制造公司在遭勒索软件攻击后工厂停产[EB/OL]. https://ti.dbappsecurity.com.cn/info/1796, 2021-03-25.

[3] 哥斯达黎加国家财政系统遭勒索攻击: 税务海关停摆[EB/OL]. https://www.freebuf.com/news/330941.html, 2022-04-25.

[4] MarketsandMarkets (2020) Managed Security Services Market Worth $46.4 Billion by 2025. India.

[5] Fortinet (2021) Cloud Security Report. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-cybersecurity-cloud-security-report-fortinet-2.5.pdf

[6] 新加坡电信巨头近 13 万客户信息遭泄露, 涉身份证号等[EB/OL]. https://3g.163.com/dy/article/G358TCLE05129QAF.html, 2021-02-19.

[7] Hoecht, A. and Trott, P. (2006) Outsourcing, Information Leakage and the Risk of Losing Technology-Based Competencies. *European Business Review*, **18**, 395-412. https://doi.org/10.1108/09555340610686967

[8] Alexander, M. and Young, D. (1996) Strategic Outsourcing. *Long Range Planning*, **29**, 116-119. https://doi.org/10.1016/0024-6301(95)00075-5

[9] Lacity, M.C. and Willcocks, L.P. (1998) An Empirical Investigation of Information Technology Sourcing Practices: Lessons from Experience. *MIS Quarterly*, **22**, 363-408. https://doi.org/10.2307/249670

[10] Lee, C.H., Geng, X.J. 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

[11] 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

[12] Varian, H. (2000) Managing Online Security Risks. *The New York Times*.

[13] 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

[14] Grossman, G.M. and Helpman, E. (2005) Outsourcing in a Global Economy. *Review of Economic Studies*, **72**, 135-159. https://doi.org/10.1111/0034-6527.00327

[15] Shy, O. and Stenbacka, R. (2005) Partial Outsourcing, Monitoring Cost, and Market Structure. *Canadian Journal of Economics/Revue Canadienne d'Économique*, **38**, 1173-1190. https://doi.org/10.1111/j.0008-4085.2005.00320.x

[16] Alvarez, L.H.R. and Stenbacka, R. (2007) Partial Outsourcing: A Real Options Perspective. *International Journal of Industrial Organization*, **25**, 91-102. https://doi.org/10.1016/j.ijindorg.2006.01.003

[17] Rowe, B.R. (2007) Will Outsourcing IT Security Lead to a Higher Social Level of Security? *Proceedings of the* 6*th*

Workshop on the Economics of Information Security, Pittsburgh, 7-8 June 2007.

[18] Wu, Y., Tayi, G.K., Feng, G. and Fung, R.Y.K. (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

[19] Cezar, A., Cavusoglu, H. and Raghunathan, S. (2014) Outsourcing Information Security: Contracting Issues and Security Implications. *Management Science*, **60**, 638-657. https://doi.org/10.1287/mnsc.2013.1763

[20] Yang, M., Jacob, V.S. and Raghunathan, S. (2020) 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

[21] 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

[22] 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

[23] Zhang, C., Feng, N., Chen, J., Li, D. and Li, M. (2020) Outsourcing Strategies for Information Security: Correlated Losses and Security Externalities. *Information Systems Frontiers*, **23**, 773-790. https://doi.org/10.1007/s10796-020-10009-4

[24] Wu, Y., Xu, M., Cheng, D. and Dai, T. (2022) Information Security Strategies for Information-Sharing Firms Considering a Strategic Hacker. *Decision Analysis*, **19**, 99-122. https://doi.org/10.1287/deca.2021.0442

[25] Miller, A. and Tucker, C. (2010) Encryption and Data Loss. *The 9th Workshop on Economics of Information Security*, Arlington, 7-8 June 2010.

[26] Ghose, A. and Rajan, U. (2006) The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare. *The 5th Workshop on Economics of Information Security*, Cambridge, 26-28 June 2006.

[27] 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

[28] Gao, X., Gong, S., Wang, Y., Wang, X. and Qiu, M. (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

[29] Smith, G. (2011) Quantifying Information Flow Using Min-Entropy. 2011 *Eighth International Conference on Quantitative Evaluation of SysTems*, Aachen, 5-8 September 2011, 159-167. https://doi.org/10.1109/QEST.2011.31

[30] Wheatman, V., Smith, B.S., Pescatore, J., Nicollet, M., Allan, A. and Mogull, R. (2005) What Your Organization Should Be Spending for Information Security.

[31] Gupta, A. and Zhdanov, D. (2012) Growth and Sustainability of Managed Security Services Networks: An Economic Perspective. *MIS Quarterly*, **36**, 1109-1130. https://doi.org/10.2307/41703500

[32] Schwartz, R. (1997) Legal Regimes, Audit Quality and Investment. *Accounting Review*, **72**, 385-406.

[33] Temizkan, O., Park, S. and Saydam, C. (2017) Software Diversity for Improved Network Security: Optimal Distribution of Software-Based Shared Vulnerabilities. *Information Systems Research*, **28**, 828-849. https://doi.org/10.1287/isre.2017.0722