E-Commerce Letters 电子商务评论, 2026, 15(3), 96-106
Published Online March 2026 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2026.153252

Hans汉斯

不确定网络安全环境下考虑制造商渠道入侵的平台供应链信息共享策略研究

张涞贤*，钟园景

西安建筑科技大学管理学院，陕西 西安

收稿日期：2026年1月21日；录用日期：2026年2月3日；发布日期：2026年3月3日

摘　要

在不确定的网络安全环境下，电商平台不仅要面对数据安全风险，还要应对上游制造商的渠道入侵，这加剧了信息共享策略的制定难度。基于此，本文针对单个制造商和单个电商平台构成的二级供应链，考虑数据安全风险传播对制造商渠道入侵下的电商平台信息共享策略的影响。研究发现：(1) 在制造商以转售形式进行渠道入侵的情形下，电商平台会隐藏信息。(2) 在制造商以代销形式进行渠道入侵的情形下，当佣金率较小且数据安全风险影响较小或佣金率较大且网络攻击造成的损失较小时电商平台会共享信息。(3) 考虑制造商渠道入侵的平台供应链，数据安全风险传播对制造商信息共享价值的负向影响大于对电商平台信息共享价值的负向影响。本文的研究结论可为不确定网络安全环境下考虑制造商渠道入侵的电商平台最优信息共享决策制定提供参考。

关键词

不确定网络安全环境，渠道入侵，平台供应链，数据安全风险传播，信息共享

Research on Platform Supply Chain Information Sharing Strategies Considering Manufacturer Channel Encroachment under Uncertain Cybersecurity Environment

Suxian Zhang*, Yuanjing Zhong

School of Management, Xi'an University of Architecture and Technology, Xi'an Shaanxi

Received: January 21, 2026; accepted: February 3, 2026; published: March 3, 2026

*通讯作者。

文章引用: 张涞贤, 钟园景. 不确定网络安全环境下考虑制造商渠道入侵的平台供应链信息共享策略研究[J]. 电子商务评论, 2026, 15(3): 96-106. DOI: 10.12677/ecl.2026.153252

Abstract

In an uncertain network security environment, e-commerce platforms not only face data security risks, but also deal with channel intrusion by upstream manufacturers, which aggravates the difficulty of formulating information sharing strategies. Based on this, this paper considers the impact of data security risk propagation on the information sharing strategy of the e-commerce platform under the manufacturer's channel intrusion for the secondary supply chain composed of a single manufacturer and a single e-commerce platform. The study found that: (1) In the case of channel intrusion by the manufacturer in the form of resale, the e-commerce platform hides information. (2) In the case of manufacturer's channel intrusion in the form of consignment, when the commission rate is low and the impact of data security risk is small or the commission rate is large and the loss caused by hacker attack is small, the e-commerce platform will share information. (3) Considering the platform supply chain with manufacturer channel intrusion, the negative impact of data security risk communication on the value of manufacturer information sharing is greater than that on the value of e-commerce platform information sharing. The research conclusions of this paper can provide reference for the optimal information sharing decision-making of e-commerce platform considering manufacturer channel intrusion under uncertain network security environment.

Keywords

Uncertain Cybersecurity Environment, Channel Encroachment, Platform Supply Chain, Data Security Risk Propagation, Information Sharing

1. 引言

在不确定的网络安全环境中，网络攻击事件频繁发生，供应链信息管理过程中的数据安全风险日益严峻[1]。更为重要的是，数据安全风险会随着信息共享进行传播，危及整个供应链的正常运营[2]。供应链中共享的信息存储在双方的服务器或云端，如果一方被网络攻击，共享的数据可能受到损害，即网络入侵一方的同时也会对其他成员造成不利影响[3]。例如，2020 年由于供应商应用程序的安全漏洞，导致亚马逊、PayPal 等知名公司的 800 万条销售记录被曝光，对相关企业造成巨大损失[4]。在不确定的网络安全环境中除数据安全风险外，电商平台还面临着来自上游制造商的渠道入侵。伴随网络经济的快速发展，越来越多的电商平台供货商开始在电商平台上为自有品牌产品开辟销售渠道[5]。例如，海尔、美的、三星等厂商在京东平台开通旗舰店，与京东自营店的同种产品“同台竞争”[6]，Silver Onyx 不仅为亚马逊平台供货，也在亚马逊平台上直接销售自有品牌产品[7]。为提高供应链效率和效益，电商平台会进行信息共享，如共享库存、销售数据和客户数据，从而提高效率和效益[8]。然而，面对不确定网络安全环境中网络攻击造成的数据安全风险传播和制造商的渠道入侵，下游电商平台应该如何制定信息共享策略？

学者们聚焦不确定网络安全环境下的数据安全问题进行了研究。部分学者研究表明企业在发生数据安全问题后，现金流波动性、信用评级下降和破产风险都会增加[9]。鉴于公众对数据安全问题的重视，供应链中的数据安全引起了学者们的关注。Crosignani 等[10]阐述了网络攻击对供应链系统的破坏性。关于数据安全对供应链安全投资决策影响的研究中，已有学者研究关注数据安全投资和安全信息共享[3]

[11]，这些研究主要关注供应链成员在面对网络攻击时所作的安全投资决策以及供应链成员之间安全信息共享对各自安全投资的影响。然而，鲜有考虑不确定网络安全环境中数据安全风险传播对制造商渠道入侵的平台供应链信息共享策略的影响。

国内外对制造商渠道入侵进行了广泛的研究。传统观点认为，制造商渠道入侵往往会对电商平台产生不利影响，电商平台隐藏信息会对自身有利[12]。在此观点基础上，部分学者拓展探究了佣金率和渠道竞争强度[6]和数据驱动营销[13]对信息共享策略的影响。上述文献主要研究上游制造商渠道入侵对下游信息共享的影响，与此不同，本文在不确定网络安全环境下，探讨数据安全风险传播和上游制造商渠道侵占对下游电商平台信息共享策略的影响。

2. 问题描述与基本假设

2.1. 问题描述

本文研究一个由制造商(用 M 表示)和电商平台(用 P 表示)组成的两级供应链，其中电商平台通过转售渠道销售自有品牌产品，电商平台以批发价格 w_1 从制造商处进货，随后以零售价格 p_1 销售给消费者。与电商平台签订了批发合同的制造商决定以转售(电商平台决定竞争型产品零售价格 p_2)或者代销(制造商决定竞争型产品零售价格 p_2，电商平台根据制造商的每笔交易收取比例为 ϕ 的佣金)形式进行渠道入侵，推出自己品牌标识的竞争型产品，该竞争型产品将与电商平台的自有品牌产品在同一市场上进行销售，两种产品之间的竞争强度用 γ 表示。电商平台接近终端市场且拥有先进的信息技术和数据分析工具，能够通过历史销售数据分析等方式更准确地了解市场需求信息，并决定是否向制造商共享市场需求信息[6]。由于网络安全环境的不确定性，制造商和电商平台均面临网络攻击。网络攻击制造商会导致市场规模降低 L_M，而攻击电商平台会导致市场规模降低 L_P。制造商和电商平台各自面临的数据安全风险会由于供应链信息共享而传播给对方。数据安全风险传播概率 $s\left(0<s<1\right)$ 由制造商和电商平台之间需求信息共享的相互信任和授权程度决定，制造商和电商平台之间的联系越紧密，数据安全风险传播概率就越大[3]。基于此，建立如图 1 所示的考虑数据安全风险传播的四种不同场景的供应链结构。

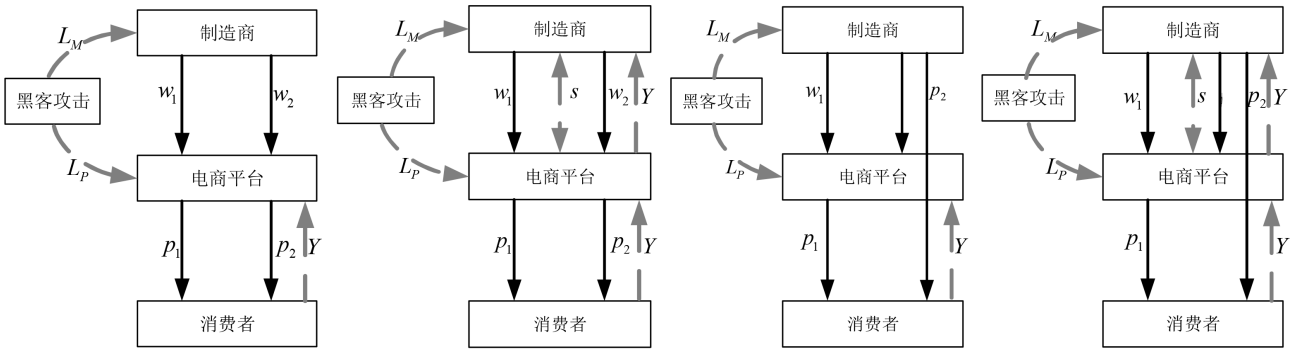


Figure 1. Supply chain model of manufacturer channel intrusion considering data security risk propagation
图 1. 考虑数据安全风险传播的制造商渠道入侵的供应链模型

2.2. 基本假设

为了便于构建数理模型，参考相关文献，结合管理实际，作出如下假设：

假设一：Dash 等[14]指出，在网络攻击情形下企业安全漏洞概率可表示为 $\rho_i\left(v,h\right)$。其中，$v_i\left(0<v<1\right)$ 表示企业信息系统的内在脆弱性，即网络攻击的成功概率；$h\left(0<h<1\right)$ 表示网络攻击概率。安全漏洞概

率 $\rho_i(v,h)$ 满足条件：$\frac{\partial \rho_i}{\partial v} \geq 0$ 且 $\frac{\partial \rho_i}{\partial h} \geq 0$。基于上述分析，网络攻击情形下的企业安全漏洞概率函数表示为 $\rho_i = hv_i, i \in (M,P)$。

假设二：网络成功入侵企业会导致市场规模降低[15]，制造商遭受网络攻击时市场规模降低 L_M，电商平台遭受网络攻击时市场规模降低 L_P，其中 $L_P = \lambda L_M$ 且 $\lambda \geq 1$ [11]，λ 表示电商平台遭受网络攻击的损失系数。一般来说，电商平台存储了消费者的大量数据，因此，相较于制造商，其遭受网络攻击会导致更严重的损失。据此可得供应链的安全状态及其市场规模如表 1 和表 2 所示：

Table 1. Supply chain security status and market size reduction in the case of hidden information
表 1. 隐藏信息情形下供应链安全状态及市场规模降低

安全状态		事件发生概率	消费者购买意愿降低
制造商未受攻击	电商平台未受攻击	$(1-\rho_M)(1-\rho_P)$	0
	电商平台受攻击	$(1-\rho_M)\rho_P$	L_P
制造商受攻击	电商平台未受攻击	$\rho_M(1-\rho_P)$	L_M
	电商平台受攻击	$\rho_M\rho_P$	$L_M + L_P$

损失期望：$\Delta^N = 0(1-\rho_M)(1-\rho_P) + L_P(1-\rho_M)\rho_P + L_M\rho_M(1-\rho_P) + (L_M+L_P)\rho_M\rho_P$，化简可得 $\Delta^N = L_M h(\lambda v_P + v_M)$。借鉴相关文献[6]，通过消费者效用函数：$\sum_{i=1,2}^{j=N,S}\left[(a+\theta-\Delta^j)q_i - \frac{q_i^2}{2} - p_i q_i\right] - \gamma q_1 q_2$，其中 a 代表市场规模的确定部分，$0<\gamma<1$ 代表产品竞争程度，在考虑消费者效用最大化情况下隐藏信息情形下的需求函数可表示为 $q_1^N = \frac{(-h(\lambda v_P + v_M)L_M + a - p_2 + \theta)\gamma + h(\lambda v_P + v_M)L_M - a + p_1 - \theta}{\gamma^2 - 1}$，$q_2^N = \frac{(-h(\lambda v_P + v_M)L_M + a - p_1 + \theta)\gamma + h(\lambda v_P + v_M)L_M - a + p_2 - \theta}{\gamma^2 - 1}$。

Table 2. Supply chain security status and market size reduction in the case of shared information
表 2. 共享信息情形下供应链安全状态及市场规模降低

安全状态		事件发生概率	消费者购买意愿降低
制造商未受攻击	电商平台未受攻击	$(1-\rho_M)(1-\rho_P)$	0
	电商平台受攻击	$(1-\rho_M)\rho_P$	$L_P + sL_P$
制造商受攻击	电商平台未受攻击	$\rho_M(1-\rho_P)$	$L_M + sL_M$
	电商平台受攻击	$\rho_M\rho_P$	$L_M + L_P + sL_M + sL_P$

损失期望：$\Delta^S = 0(1-\rho_M)(1-\rho_P) + (L_P+sL_P)(1-\rho_M)\rho_P + (L_M+sL_M)\rho_M(1-\rho_P) + (L_M+L_P+sL_M+sL_P)\rho_M\rho_P$，化简可得 $\Delta^S = L_M h(\lambda v_P + v_M)(s+1)$。借鉴相关文献[6]，通过消费者效用函数：$\sum_{i=1,2}^{j=N,S}\left[(a+\theta-\Delta^j)q_i - \frac{q_i^2}{2} - p_i q_i\right] - \gamma q_1 q_2$，在考虑消费者效用最大化情况下共享信息情形下的需求函数可表

示为 $q_1^S=\frac{\left(-h(s+1)(\lambda v_P+v_M)L_M+a+\theta-p_2\right)\gamma+h(s+1)(\lambda v_P+v_M)L_M-a-\theta+p_1}{\gamma^2-1}$，

$q_2^S=\frac{\left(-h(s+1)(\lambda v_P+v_M)L_M+a+\theta-p_1\right)\gamma+h(s+1)(\lambda v_P+v_M)L_M-a-\theta+p_2}{\gamma^2-1}$。

假设三：基于大量的消费者购物数据和大数据分析技术，电商平台能够预测市场需求不确定性水平 θ 的私有信号 Y [5] [16]，假设 Y 是 θ 的无偏估计值，即 $E[Y|\theta]=\theta$ 且 θ 的期望以 Y 为条件，与 Y 成线性关系，如下所示：

$$E[\theta|Y]=\frac{1}{1+t\sigma^2}E[\theta]+\frac{t\sigma^2}{1+t\sigma^2}Y=\frac{t\sigma^2}{1+t\sigma^2}Y$$

其中 $t=\frac{1}{E[Var[Y|\theta]]}$ 代表预测精度。$t=0$ 时，需求预测精度为 0，$E[\theta|Y]=0$。当 $t\to+\infty$ 时，电商平台具备完全的需求信息预测能力。为便于计算，令 $\beta(t,\sigma)=\frac{t\sigma^2}{1+t\sigma^2}$。

3. 模型求解与分析

3.1. 制造商以转售形式进行渠道入侵且电商平台隐藏信息的情形(RN)

在 RN 情形下，在电商平台以转售渠道销售自有品牌产品基础上，制造商以转售形式进行渠道入侵，且电商平台不向制造商共享需求信息。双方均以利润最大化为目标，制造商先制定批发价格 w_1 和 w_2，电商平台据此再制定零售价格 p_1 和 p_2。制造商和电商平台的目标函数如下所示：

$$\max_{w_1,w_2}E\left[\pi_M^{RN}\right]=E\left[w_1q_1^N+w_2q_2^N\right] \tag{1}$$

$$\max_{p_1,p_2}E\left[\pi_P^{RN}|Y\right]=E\left[(p_1-w_1)q_1^N+(p_2-w_2)q_2^N|Y\right] \tag{2}$$

通过逆向归纳法，求解 RN 情形下制造商和电商平台的均衡决策，可得命题 1。

命题 1：在 RN 情形下，制造商的均衡批发价格 $w_1^{RN*}=w_2^{RN*}=-\frac{h(\lambda v_P+v_M)L_M}{2}+\frac{a}{2}$，电商平台的均衡零售价格 $p_1^{RN*}=p_2^{RN*}=-\frac{3h(\lambda v_P+v_M)L_M}{4}+\frac{\beta Y}{2}+\frac{3a}{4}$，双方的事前利润分别为 $E\left[\pi_M^{RN}\right]=\frac{\left(-h(\lambda v_P+v_M)L_M+a\right)^2}{4\gamma+4}$ 和 $E\left[\pi_P^{RN}\right]=\frac{\beta\sigma^2}{2(\gamma+1)}+\frac{\left(L_Mh\lambda v_P+L_Mhv_M-a\right)^2}{8(\gamma+1)}$。

3.2. 制造商以转售形式进行渠道入侵且电商平台共享信息的情形(RS)

在 RS 情形下，在电商平台以转售渠道销售自有品牌产品基础上，制造商以转售形式进行渠道入侵，且电商平台向制造商共享需求信息。双方均以利润最大化为目标，制造商先制定批发价格 w_1 和 w_2，电商平台据此再制定零售价格 p_1 和 p_2。制造商和电商平台的目标函数如下所示：

$$\max_{w_1,w_2}E\left[\pi_M^{RS}|Y\right]=E\left[w_1q_1^S+w_2q_2^S|Y\right] \tag{3}$$

$$\max_{p_1,p_2}E\left[\pi_P^{RS}|Y\right]=E\left[(p_1-w_1)q_1^S+(p_2-w_2)q_2^S|Y\right] \tag{4}$$

通过逆向归纳法，求解 RS 情形下制造商和电商平台的均衡决策，可得命题 2。

命题 2：在 RS 情形下，制造商的均衡批发价格 $w_1^{RS*}=w_2^{RS*}=-\frac{h(s+1)(\lambda v_P+v_M)L_M}{2}+\frac{a}{2}+\frac{\beta Y}{2}$，电商

平台的均衡零售价格 $p_1^{RS*}=p_2^{RS*}=-\frac{3h(s+1)(\lambda v_P+v_M)L_M}{4}+\frac{3\beta Y}{4}+\frac{3a}{4}$，双方的事前利润分别为 $E\left[\pi_M^{RS}\right]=\frac{\beta\sigma^2+\left(h(\lambda v_P+v_M)(s+1)L_M-a\right)^2}{4\gamma+4}$ 和 $E\left[\pi_P^{RS}\right]=\frac{\beta\sigma^2+\left(h(\lambda v_P+v_M)(s+1)L_M-a\right)^2}{8\gamma+8}$。

3.3. 制造商以代销形式进行渠道入侵且电商平台隐藏信息的情形(AN)

在 AN 情形下，在电商平台以转售渠道销售自有品牌产品基础上，制造商以代销形式进行渠道入侵，且电商平台不向制造商共享需求信息。双方均以利润最大化为目标，制造商先制定批发价格 w_1 和零售价格 p_2，电商平台据此再制定零售价格 p_1。制造商和电商平台的目标函数如下所示：

$$\max_{w,p_2} E\left[\pi_M^{AN}\right]=E\left[w_1q_1^N+(1-\phi)p_2q_2^N\right] \tag{5}$$

$$\max_{p_1} E\left[\pi_P^{AN}\mid Y\right]=E\left[(p_1-w_1)q_1^N+\phi p_2q_2^N\mid Y\right] \tag{6}$$

通过逆向归纳法，求解 AN 情形下制造商和电商平台的均衡决策，可得命题 3。

命题 3：在 AN 情形下，制造商的均衡批发价格 $w_1^{AN*}=-\frac{(\gamma\phi-1)\left(-h(\lambda v_P+v_M)L_M+a\right)}{2}$，均衡代销价格 $p_2^{AN*}=-\frac{h(\lambda v_P+v_M)L_M}{2}+\frac{a}{2}$，电商平台的均衡零售价格 $p_1^{AN*}=\frac{\left(h(\lambda v_P+v_M)L_M-2\beta Y-a\right)\gamma-3h(\lambda v_P+v_M)L_M}{4}+\frac{\beta Y}{2}+\frac{3a}{4}$，双方的事前利润分别为 $E\left[\pi_M^{AN}\right]=-\frac{2\left(\left(\phi-\frac{1}{2}\right)\gamma+\phi-\frac{3}{2}\right)\left(-h(\lambda v_P+v_M)L_M+a\right)^2}{8\gamma+8}$ 和 $E\left[\pi_P^{AN}\right]=\frac{(\gamma-1)\beta\sigma^2}{4(\gamma+1)}+\frac{(4\gamma\phi-\gamma+4\phi+1)\left(L_Mh\lambda v_P+L_Mhv_M-a\right)^2}{16(\gamma+1)}$。

3.4. 制造商以代销形式进行渠道入侵且电商平台共享信息的情形(AS)

在 AS 情形下，在电商平台以转售渠道销售自有品牌产品基础上，制造商以代销形式进行渠道入侵，且电商平台向制造商共享需求信息。双方均以利润最大化为目标，制造商先制定批发价格 w_1 和零售价格 p_2，电商平台据此再制定零售价格 p_1。制造商和电商平台的目标函数如下所示：

$$\max_{w,p_2} E\left[\pi_M^{AS}\mid Y\right]=E\left[w_1q_1^S+(1-\phi)p_2q_2^S\mid Y\right] \tag{7}$$

$$\max_{p_1} E\left[\pi_P^{AS}\mid Y\right]=E\left[(p_1-w_1)q_1^S+\phi p_2q_2^S\mid Y\right] \tag{8}$$

通过逆向归纳法，求解 AS 情形下制造商和电商平台的均衡决策，可得命题 4。

命题 4：在 AS 情形下，制造商的均衡批发价格 $w_1^{AS*}=-\frac{(\gamma\phi-1)\left(-h(s+1)(\lambda v_P+v_M)L_M+\beta Y+a\right)}{2}$，均衡代销价格 $p_2^{AS*}=-\frac{h(s+1)(\lambda v_P+v_M)L_M}{2}+\frac{\beta Y}{2}+\frac{a}{2}$，电商平台的均衡零售价格 $p_1^{AS*}=-\frac{\left(-h(s+1)(\lambda v_P+v_M)L_M+\beta Y+a\right)(\gamma-3)}{4}$，双方的事前利润分别为 $E\left[\pi_M^{AS}\right]=-\frac{(2\gamma\phi-\gamma+2\phi-3)\left[\beta\sigma^2+\left(L_Mh\lambda sv_P+L_Mh\lambda v_P+L_Mhsv_M+L_Mhv_M-a\right)^2\right]}{8(\gamma+1)}$ 和

$$E\left[\pi_P^{AS}\right]=\frac{\left(4\gamma\phi-\gamma+4\phi+1\right)\left[\beta\sigma^2+\left(L_M h\lambda s v_P+L_M h\lambda v_P+L_M h s v_M+L_M h v_M-a\right)^2\right]}{16\left(\gamma+1\right)}。$$

4. 均衡信息共享策略分析

在不确定的网络安全环境下，考虑制造商以转售形式进行渠道入侵，制造商和电商平台信息共享策略如引理 1 所示。

引理 1：(a) 当 $0<s<s_4$ 或 $s_4<s<1$ 且 $0<L_M<L_{M1}$ 时，制造商愿意获取信息。(b) 电商平台始终选择隐藏信息。其中 $s_4=\frac{2\beta\sigma^2}{-\sigma^2\beta+a^2}$，$L_{M1}=\frac{as-\sqrt{-\beta s^2\sigma^2+a^2s^2-2\sigma^2 s\beta}}{s\left(s+2\right)\left(\lambda v_P+v_M\right)h}$。

不存在数据安全风险传播时，平台供应链处于安全的网络环境。根据 Gong 等[5]关于平台供应链信息共享策略的研究可得，在制造商以转售形式进行渠道入侵的平台供应链中，制造商的信息获取策略为无条件获取需求信息，电商平台信息共享策略为隐藏需求信息。

命题 7：将本研究中的信息共享策略与 Gong 等[5]关于平台供应链信息共享策略的研究对比可得：(a) 制造商信息获取策略由无条件获取信息转变为在数据安全风险传播概率较小或数据安全风险传播概率较大且市场降低规模较小时，制造商获取需求信息。(b) 电商平台的信息共享策略与供应链均衡信息共享策略不受数据安全风险传播概率的影响，即隐藏需求信息。

命题 7 表明，在制造商以转售渠道入侵情形下，制造商信息获取策略受数据安全风险传播的影响发生变化，而电商平台信息共享策略和供应链均衡信息共享策略不受数据安全风险传播概率的影响。具体而言，命题 7(a)表明，风险传播的“风险溢出效应”与信息获取的“信息价值效应”相互制衡，进而影响双重边际效应。制造商获取需求信息可通过调整批发价增利、缓解双重边际效应，但需承担平台信息共享带来的风险损失，从而加重了双重边际效应。这种制衡决定了制造商的选择性策略：风险概率低时，信息价值效应主导，制造商获取信息；风险概率高但市场降幅小时，信息价值仍能覆盖风险成本，制造商仍选择获取；若风险高且市场降幅显著，风险效应抵消信息价值，制造商放弃获取。命题 7(b)表明，电商平台的信息共享决策始终以自身利益为核心，与风险传播概率无关。需求信息是平台核心优势，共享信息会使其丧失壁垒、承担风险反向传播成本，损害自身经营。因此无论风险概率高低，平台共享信息均无收益且需承担损失，还会加剧双重边际效应，因此始终选择隐藏信息。

在不确定的网络安全环境下，考虑制造商以代销形式进行渠道入侵，制造商和电商平台信息共享策略如引理 2 所示。

引理 2：(a) 当 $0<s<s_4$ 或 $s_4<s<1$ 且 $0<L_M<L_{M1}$ 时，制造商获取信息。(b) 当满足以下条件时电商平台共享信息：1. 当 $0<\phi<\phi_1$ 时：$0<s<s_5$ 或 $s_5<s<1$，$0<L_M<L_{M2}$；2. 当 $\phi_2<\phi<\phi_3$ 时：$0<L_M<L_{M2}$。其中 $\phi_1=\frac{9\beta\gamma\sigma^2+a^2\gamma-9\beta\sigma^2-a^2}{4\left(-3\beta\gamma\sigma^2+a^2\gamma-3\beta\sigma^2+a^2\right)}$，$\phi_2=\frac{3\beta\gamma\sigma^2+a^2\gamma-3\beta\sigma^2-a^2}{4\left(-\beta\gamma\sigma^2+a^2\gamma-\beta\sigma^2+a^2\right)}$，$\phi_3=-\frac{3\left(\gamma-1\right)}{4\left(\gamma+1\right)}$，$\phi_1<\phi_2<\phi_3$，

$$s_5=\frac{2\beta\sigma^2\left(4\gamma\phi+3\gamma+4\phi-3\right)}{-4\beta\gamma\phi\sigma^2+4a^2\gamma\phi-3\beta\gamma\sigma^2-4\beta\phi\sigma^2-a^2\gamma+4a^2\phi+3\beta\sigma^2+a^2}，$$

$$L_{M2}=\frac{\left(\begin{array}{l}2s\left(\lambda v_P+v_M\right)a\left(4\gamma\phi-\gamma+4\phi+1\right)h\\-2\sqrt{\begin{array}{l}s^2\left(\lambda v_P+v_M\right)^2a^2\left(4\gamma\phi-\gamma+4\phi+1\right)^2h^2\\-s\left(\lambda v_P+v_M\right)^2\left(s+2\right)\left(4\gamma\phi-\gamma+4\phi+1\right)h^2\left(4\gamma\phi+3\gamma+4\phi-3\right)\beta\sigma^2\end{array}}\end{array}\right)}{2s\left(\lambda v_P+v_M\right)^2\left(s+2\right)\left(4\gamma\phi-\gamma+4\phi+1\right)h^2}。$$

不存在数据安全风险传播时，平台供应链处于安全的网络环境。根据 Gong 等[5]和 Ha 等[6]关于平台供应链信息共享策略的研究可得，在制造商以代销形式进行渠道入侵的平台供应链中，制造商的信息获取策略为无条件获取需求信息，电商平台信息共享策略为在佣金率较大时共享需求信息。

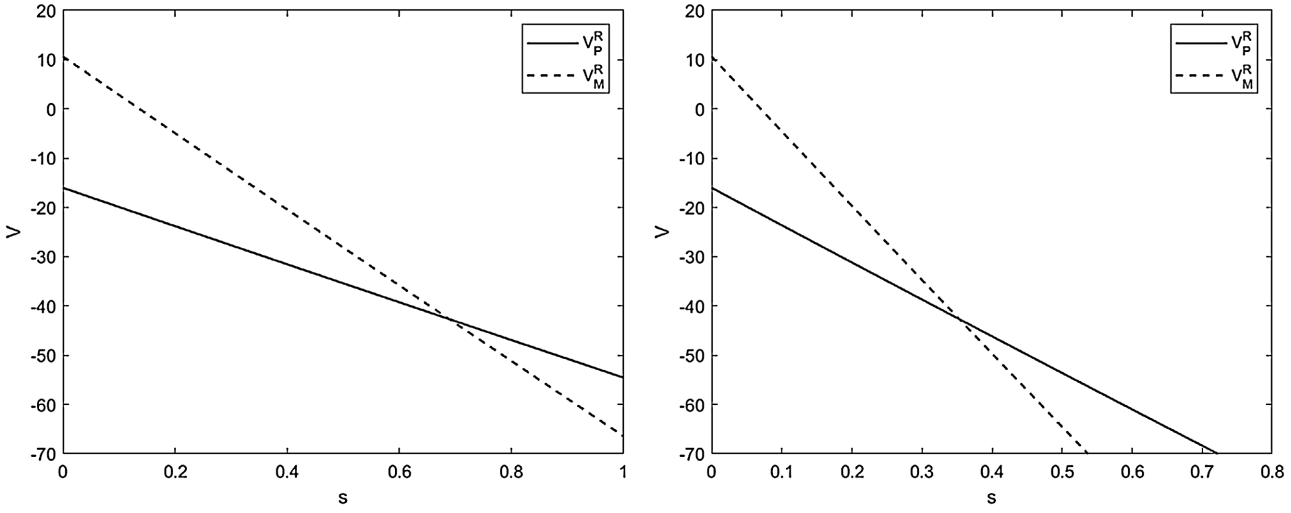
命题 8：将本研究中的信息共享策略与 Gong 等[5]关于平台供应链信息共享策略的研究对比可得：(a) 制造商信息获取策略由无条件获取信息转变为当数据安全风险传播概率较小或数据安全风险传播概率较大且市场降低规模较小时，制造商获取需求信息。(b) 电商平台信息共享策略由仅在佣金率较大时共享需求信息转变为当佣金率较小时，数据安全风险传播概率较小或数据安全风险传播概率较大但网络攻击造成的损失较小；当佣金率较大且网络攻击造成的损失较小时，电商平台共享需求信息。

命题 8 表明，在制造商以代销形式进行渠道入侵的情形下，制造商信息获取策略、电商平台信息共享策略和供应链均衡信息共享策略受数据安全风险传播概率的影响发生改变。具体而言，如命题 8(a)所示，受数据安全风险传播的影响，在制造商以代销渠道入侵的平台供应链中，制造商在数据安全风险传播概率较小或数据安全风险传播概率较大且市场降低规模较小时获取信息。命题 8(a)与命题 7(a)逻辑一致，核心差异在于场景为代销渠道入侵：受风险溢出效应与信息价值效应制衡，制造商仅在风险可控范围内获取信息。当风险传播概率低，或概率高但市场降幅小时，制造商承担的风险处于可承受范围，信息价值效应覆盖风险成本，因此愿意获取需求信息；反之则放弃。如命题 8(b)所示，受数据安全风险传播的影响，在制造商以代销渠道入侵的平台供应链中，当佣金率较小时数据安全风险传播概率较小或数据安全风险传播概率较大但网络攻击造成的损失较小时、当佣金率较大且网络攻击造成的损失较小时，电商平台共享信息。原因在于，电商平台的共享策略受佣金率、风险传播概率及网络攻击损失的共同影响，本质是信息共享正效应与风险负效应的制衡结果。当佣金率小时，平台代销利润有限，仅在风险可控(传播概率低，或概率高但网络损失小)时，风险负效应低于信息共享正效应，平台愿意共享；当佣金率大时，平台代销利润丰厚，只要网络攻击损失小，信息共享正效应(进一步提升收益)便会覆盖风险负效应，因此平台愿意共享信息。

5. 数据安全风险传播概率对信息共享价值的影响

本章通过数值分析方法来探寻表征不确定网络安全环境的主要参数对制造商和电商平台利润的影响。借鉴 Xu 等[3]和 Chen 等[12]的研究，相关参数赋值如下：$a=100$，$v_P=0.8$，$v_M=0.8$，$\lambda=1$，$h=0.3$，$s=0.4$，$\beta=1$，$\sigma=8$，$\phi=0.3$，$\gamma=0.5$。图 2 和图 3 分别反映了数据安全风险传播概率对信息共享价值的影响规律，其中 $V_i^R\ (i\in(M,P))$ 表示制造商以转售形式进行渠道入侵情形下的信息共享价值，$V_i^A\ (i\in(M,P))$ 表示制造商以代销形式进行渠道入侵情形下的信息共享价值。图 2 和图 3 中各有两个子图，以区别在 L_M 变化时，数据安全风险传播概率对于制造商和电商平台信息共享价值的影响。

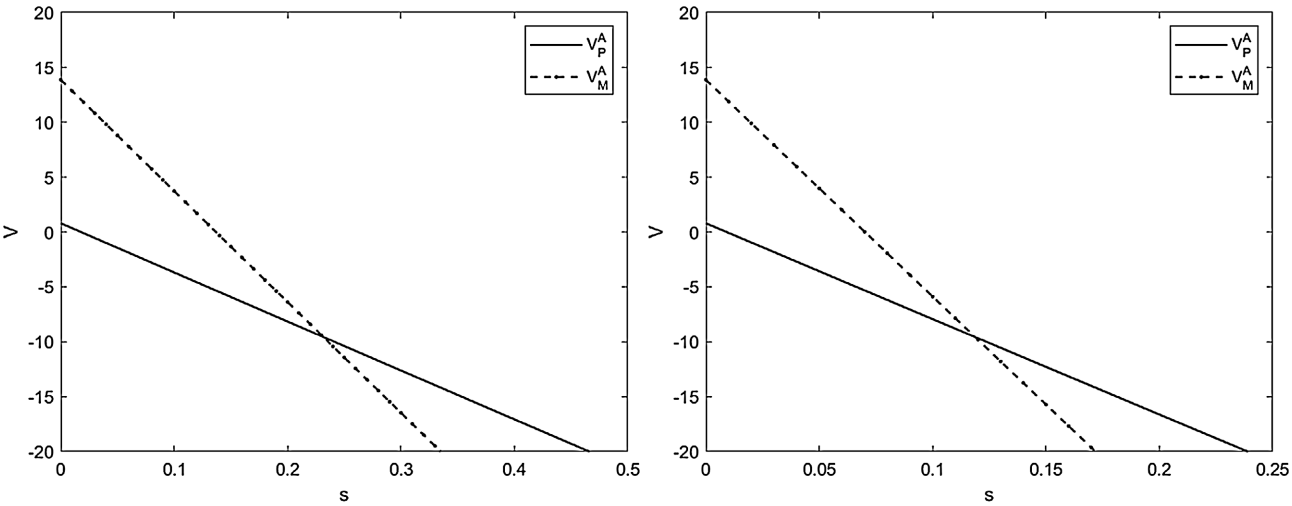
如图 2 和图 3 所示，随着数据安全风险传播概率的增大，制造商和电商平台的信息共享价值逐渐减小。即数据安全风险传播概率对制造商和电商平台的信息共享价值具有负向影响。通过对比图 2 和图 3 中实线和虚线的斜率可知，虚线的斜率大于实线的斜率，这表明随着数据安全风险传播概率的增大，制造商信息共享价值的减少幅度大于电商平台信息共享价值的减少幅度。换言之，数据安全风险传播概率对制造商信息共享价值的负向影响大于对电商平台的信息共享价值的负向影响。原因在于，在不确定的网络安全环境中电商平台遭受网络攻击时的损失大于制造商遭受网络攻击时的损失，因此电商平台向制造商传递的数据安全风险大于制造商向电商平台传递的数据安全风险。换言之，在信息共享过程中制造商相较于电商平台面临着更大的数据安全风险。



(a) $L_M = 5$ (b) $L_M = 10$

Figure 2. The impact of data security risk propagation probability on the value of information sharing in the case of manufacturer's resale channel invasion

图 2. 制造商以转售渠道入侵情形下数据安全风险传播概率对信息共享价值的影响



(a) $L_M = 5$ (b) $L_M = 10$

Figure 3. The impact of data security risk propagation probability on the value of information sharing in the case of manufacturer's consignment channel intrusion

图 3. 制造商以代销渠道入侵情形下数据安全风险传播概率对信息共享价值的影响

6. 结语

本文在不确定网络安全环境中构建考虑制造商渠道入侵的平台供应链信息共享决策模型，探讨数据安全风险传播对制造商渠道入侵情形下电商平台信息共享策略的影响，进而剖析数据安全风险传播在制造商以不同形式进行渠道入侵情形下对电商平台信息共享策略的差异化影响。本文的主要研究结论为：

(1) 在制造商以转售形式进行渠道入侵的情形下，电商平台选择隐藏信息，这与 Gong 等[5]的研究结论相似。然而，考虑数据安全风险传播和制造商以转售形式进行渠道入侵情形下电商平台信息共享并不总是有利于制造商。(2) 在制造商以代销形式进行渠道入侵情形下，电商平台选择在一定条件下共享信息，这与 Gong 等[5]的研究结论具有差异。具体而言，与安全的网络环境下电商平台仅在代销渠道佣金率较

高时共享信息不同的是，当佣金率较小且数据安全风险影响较小或佣金率较大且网络攻击造成的损失较小时，电商平台会共享信息。(3) 数据安全风险传播对制造商信息共享价值的负向影响大于对电商平台信息共享价值的负向影响。

基于上述研究结论，可以得到以下管理启示：(1) 对于制造商而言，在接受来自电商平台共享的需求信息时，不仅需要关注信息共享所带来的信息优势，同时需要关注信息共享过程中数据安全风险传播的不利影响。(2) 对于电商平台而言，在制造商以代销渠道入侵的平台供应链中，关注代销渠道佣金率的变化的同时需要同时关注数据安全风险传播概率的变化以调整信息共享策略。

本文以平台供应链中制造商在电商平台原有品牌基础上销售竞争型产品作为研究基础，未来研究可针对制造商开辟直销渠道或通过直播电商平台销售竞争型产品拓展研究。此外，电商平台也可能分别预测两个渠道的未来市场需求，后续研究可以在电商平台在分别预测两个渠道未来市场需求基础上研究数据安全风险传播对电商平台信息共享策略的影响。

参考文献

[1] Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., *et al.* (2021) Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture. *Sensors*, **21**, Article 6057. https://doi.org/10.3390/s21186057

[2] Deane, J., Baker, W. and Rees, L. (2022) Cybersecurity in Supply Chains: Quantifying Risk. *Journal of Computer Information Systems*, **63**, 507-521. https://doi.org/10.1080/08874417.2022.2081882

[3] Xu, L., Li, Y., Lin, Y., Tang, C. and Yao, Q. (2023) Supply Chain Cybersecurity Investments with Interdependent Risks under Different Information Exchange Modes. *International Journal of Production Research*, **62**, 2034-2059. https://doi.org/10.1080/00207543.2023.2206923

[4] ISBuzz Team (2020) 8 Million UK Shopping Records Exposed. https://informationsecuritybuzz.com/8-million-uk-shopping-records-exposed/

[5] Gong, C., Ignatius, J., Song, H., Chai, J. and Day, S.J. (2024) The Impact of Platform's Information Sharing on Manufacturer Encroachment and Selling Format Decision. *European Journal of Operational Research*, **317**, 141-155. https://doi.org/10.1016/j.ejor.2024.03.036

[6] Ha, A.Y., Luo, H. and Shang, W. (2022) Supplier Encroachment, Information Sharing, and Channel Structure in Online Retail Platforms. *Production and Operations Management*, **31**, 1235-1251. https://doi.org/10.1111/poms.13607

[7] (2021) Today at Amazon Accelerate: Amazon Announces Product Opportunity Explorer to Help Third-Party Sellers Identify New Products to Sell in Amazon's Store. https://press.aboutamazon.com/2021/10/today-at-amazon-accelerate-amazon-announces-product-opportunity-explorer-to-help-third-party-sellers-identify-new-products-to-sell-in-amazons-store

[8] Colicchia, C., Creazza, A., Noè, C. and Strozzi, F. (2019) Information Sharing in Supply Chains: A Review of Risks and Opportunities Using the Systematic Literature Network Analysis (SLNA). *Supply Chain Management*: *An International Journal*, **24**, 5-21. https://doi.org/10.1108/scm-01-2018-0003

[9] Kamiya, S., Kang, J., Kim, J., Milidonis, A. and Stulz, R.M. (2021) Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms. *Journal of Financial Economics*, **139**, 719-749. https://doi.org/10.1016/j.jfineco.2019.05.019

[10] Crosignani, M., Macchiavelli, M. and Silva, A.F. (2023) Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains. *Journal of Financial Economics*, **147**, 432-448. https://doi.org/10.1016/j.jfineco.2022.12.002

[11] Li, Y. and Xu, L. (2020) Cybersecurity Investments in a Two-Echelon Supply Chain with Third-Party Risk Propagation. *International Journal of Production Research*, **59**, 1216-1238. https://doi.org/10.1080/00207543.2020.1721591

[12] Chen, K., Liu, J., Huang, Z. and Wang, S. (2024) Information Sharing Strategy and Channel Selection with Substitutable Products. *International Journal of Production Economics*, **268**, Article ID: 109129. https://doi.org/10.1016/j.ijpe.2023.109129

[13] 尤明钏, 张智勇, 石永强. 数据驱动营销使能下信息共享与渠道扩张策略研究[J]. 管理学报, 2025, 22(5): 928-937.

[14] Dash, A., Sarmah, S.P., Tiwari, M.K., Jena, S.K. and Glock, C.H. (2024) Cybersecurity Investments in Supply Chains

with Two-Stage Risk Propagation. *Computers & Industrial Engineering*, **197**, Article ID: 110519. https://doi.org/10.1016/j.cie.2024.110519

[15] 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

[16] 王文隆, 姚锐, 张涑贤. 考虑制造商创新的供应链双向需求信息共享研究[J]. 中国管理科学, 2022, 30(5): 226-235.