地方政府互联网信息风险治理、信息成本与企业专业化分工

江沐子[1]，逯　东[2]，陈　莹[2]
（1. 四川开放大学 经济管理学院，四川 成都 610021；2. 西南财经大学 会计学院，四川 成都 611130）

摘　要：数字经济环境下，互联网信息风险呈现出传播碎片化与技术复杂化并存的特征，对地方政府治理营商网络信息环境提出了更高要求。文章基于预防性治理、即时性治理与结果性治理三个维度，构建了地方政府互联网信息风险治理水平指标体系，并从信息成本视角考察了其对企业专业化分工的影响机制。研究发现，地方政府互联网信息风险治理能够显著促进企业专业化分工，主要通过有效降低企业在交易关系构建阶段与交易关系维护阶段所面临的信息成本实现。异质性分析表明，地方政府在治理协同性、治理效率与治理威慑力方面的提升有助于增强互联网信息风险治理的整体成效；此外，在市场竞争比较激烈、企业对外部信息依赖程度较高的行业中，这一治理效应更加显著。文章在理论上拓展了信息风险视角下分工与信息成本之间的经济逻辑，在实践上为地方政府评估营商网络信息环境质量，进而推动全国统一大市场建设提供了有益的政策启示。

关键词：互联网信息风险治理；信息成本；专业化分工
中图分类号：F272　　**文献标识码：**A　　**文章编号：**1001-9952（2026）05-0035-15
DOI: 10.16538/j.cnki.jfe.20250624.102

一、引　言

在全球新发展格局下，互联网平台因高度集聚敏感数据与关键资源，成为信息风险攻击的主要载体。随着数据要素在企业运营中的深度嵌入，互联网信息风险呈现高度外部化、系统化趋势，涵盖网络瘫痪、数据泄露、非法访问、交易欺诈、虚假信息传播以及流量造假等多重威胁，严重冲击企业稳定运行和专业化协作体系。在此背景下，企业的专业化分工模式面临严峻挑战。例如，某快递物流企业因温控数据共享风险被迫收缩合作网络，转向自建闭环冷链体系，使得运输成本增加；某锂电池隔膜企业因网络谣言被迫暂停与合作方的联合研发项目，导致研发周期延长；某医药企业子公司因跨境支付诈骗事件，被迫终止与第三方支付平台合作，改为组建自营跨境支付团队，这增加了财务处理时间与管理成本，弱化了分工协作效能。这些案例表明，信息风险不仅破坏了分工协作的信任基础，导致产业链出现“逆专业化”现象，更抑制了数字技术本应带来的分工深化红利。

收稿日期：2025-01-08
基金项目：国家自然科学基金面上项目“数字经济下互联网信息生态风险治理、信息环境与企业经营效率”（72472130）
作者简介：江沐子（1996－），女，四川成都人，四川开放大学经济管理学院讲师，管理学博士；
逯　东（1981－）（通讯作者），男，四川达州人，西南财经大学会计学院教授，博士生导师；
陈　莹（1999－），女，河南三门峡人，西南财经大学会计学院博士研究生。

然而，企业在应对互联网信息犯罪及其相关的黑色产业链时面临信息孤岛、资金技术不足以及防护意识薄弱等问题（甄杰等，2020）。Posey 等（2015）指出，部分管理者认为“追求绩效”与“追求安全”之间存在目标冲突，企业进行信息安全建设无法产生直接收益。这使得单纯依赖市场机制难以有效应对信息风险潜在的负面影响（Scott，1997）。在全球信息安全治理体系尚未完全统一的情况下，国家层面治理策略发挥着关键作用。North（1990）的制度变迁理论强调，有效的制度安排有助于削减交易中的“非生产性损耗”，提高市场分工效率。地方政府互联网信息风险治理的独特价值正是在于通过制度性公共品的供给，重塑企业间信任传导链，使“风险可控—分工深化”的良性循环突破“安全—效率”的二元悖论。当前学界尚缺乏系统化的信息风险识别与治理框架，亦缺乏评估地方政府互联网信息风险治理水平的有效量化指标。因此，探讨政府如何通过信息风险治理影响企业间的专业化分工，有助于为破解数字经济下企业分工弱化困境提供新的分析维度。

需要指出的是，互联网信息风险治理的属地化实践为本文分析地方政府互联网信息风险治理成效提供了重要的依据。自《中华人民共和国网络安全法》颁布以来，《网络信息内容生态治理规定》《中华人民共和国数据安全法》《中华人民共和国反电信网络诈骗法》《网站平台受理处置涉企网络侵权信息举报工作规范》等法律法规陆续出台，构建了多维度的信息风险治理框架。与此同时，国家持续推进“净网”“剑网”等互联网生态治理专项行动，部分省市积极推动建立网络安全应急机制与专责机构，设立互联网信息风险监测平台，逐步构建起具有区域特色的治理体系。例如，广州联合阿里打击互联网“黑灰”产业，杭州打造直播电商治理平台，三亚与安恒信息合作推动本地信息安全体系建设，温州试点网络生态综合治理机制，上海发起成立威胁数据共享联盟。[①]这些实践不仅体现了地方政府由被动响应向主动治理的转变，也揭示了企业面临的信息风险治理环境具有显著的地区差异。本文的研究贡献体现在：

第一，在研究视角方面，本文基于信息风险治理视角，拓展了数字环境下影响企业决策行为的研究路径。现有研究多聚焦于国家层面的智慧城市建设或网络基础设施供给，强调提升“物理层”信息可达性以优化企业资源配置与提升经营效率（沈坤荣等，2023），其关注核心在于信息获取效率。而本文聚焦于信息的可信性与安全性，强调信息风险治理能力在保障企业交易安全与合作稳定性中的作用。本文通过将数据信息安全风险、平台内容传输风险与网络交易欺诈风险纳入统一分析框架，系统分析了企业在构建高质量专业化分工体系中面临的技术性、社会性与经济性信息环境障碍。该视角不仅弥补了现有研究对信息基础设施“硬件效应”的过度依赖以及对制度性信息治理差异的忽视，也为理解数字时代信息风险如何嵌入企业组织边界与交易模式提供了新的理论路径。

第二，在理论构建方面，本文从交易关系构建和维护两阶段细化企业面临的信息成本类型，丰富了交易成本理论在企业专业化分工研究中的运用。交易成本理论最早由 Coase（1937）提出，后由 Williamson（1979）细化为资产专用性、不确定性与交易频率三个关键维度，成为解释企业组织形式与分工决策的重要理论基础（Walker 和 Weber，1984；Acemoglu 等，2010；Mizutani 等，2015）。本文在此基础上划分的信息成本类型分别对应合作初期的识别筛选障碍与合作过程中的摩擦。这种阶段性划分不仅契合 Williamson（1985）提出的交易过程分解逻辑，也更贴合数

① 资料来源：http://it.people.com.cn/GB/n1/2016/0325/c1009-28225726.html；https://news.66wz.com/system/2018/06/04/105088501.shtml；https://www.hangzhou.gov.cn/art/2025/7/3/art_812262_59114725.html；https://baijiahao.baidu.com/s?id=1686375154218535656&wfr=spider&for=pc；https://tech.sina.com.cn/i/2019-03-22/doc-ihtxyzsk9650573.shtml。

字环境下企业面临的信息筛选难度与互动复杂性，拓展了交易成本理论在信息风险治理情境下的应用边界。

第三，在实践意义层面，本文构建了契合数字经济特征的治理指标体系，从预防性、即时性、结果性治理三个维度系统评估了政府在互联网信息风险治理中的履职效能。该体系不仅回应了数字环境下对新型治理能力的现实需求，也为地方政府整治平台经济中的黑灰产业链、遏制不正当竞争，进而推进全国统一大市场建设提供了治理参考。

二、理论分析与研究假说

数字经济在推动信息大规模生成与智能化应用的同时，也带来了贯穿数据全生命周期（如生成、存储、传输等）以及平台交互过程（如内容传播、网络交易等）的信息风险，显著加剧了市场信息摩擦。在这个背景下，地方政府互联网信息风险治理通过调节企业面临的外部交易成本和内部管控成本，重塑了企业在市场购买和自主生产之间的组织决策逻辑（Williamson，1985）。具体而言，地方政府互联网信息风险治理可通过双重路径影响企业成本结构：一是提升市场信息可靠性与交互安全性，降低市场交易成本；二是为企业提供信息安全建设、数据风险防控以及网络安全监管等技术支持，缓解企业内部管控压力，降低内部管控成本。上述两类成本调整的相对幅度决定企业的分工决策：当前者降幅更大时，企业倾向于采用市场机制实现专业化分工；反之，则倾向于纵向一体化。据此，本文从市场交易成本与内部管控成本两个维度构建理论分析框架，系统探讨地方政府互联网信息风险治理对企业组织方式选择的作用机制及情境异质性。

（一）市场交易成本主导型作用路径

当地方政府互联网信息风险治理带来的市场交易成本下降幅度超过内部管控成本的变化幅度时，企业倾向于突破组织边界，转向基于市场机制的专业化分工。从交易流程看，市场交易中的信息成本主要集中在交易关系建立与维护两个阶段，直接影响企业外部合作的可能性与效率。

一方面，在交易关系构建阶段，信息成本主要体现在企业筛选可信交易对象、验证其资信状况与履约能力所需的时间与资源投入上。尽管互联网技术拓宽了中间品供给信息的覆盖范围（施炳展和李建桐，2020），但信任机制缺失导致“数据信任赤字”问题突出（Redman，2013）。例如，部分企业通过发布虚假评论、制造负面舆论等方式误导市场认知（Cao 等，2021），加剧信息失真，迫使企业投入大量资源甄别信息，推高了前期合作的试错成本。对此，地方政府通过建设智能化信息风险监测体系、实时筛查“虚假宣传”“网络刷单”等行为，提升了企业资信状况、历史履约记录等关键数据的透明度与可验证性。这种制度性信息净化机制降低了识别优质交易对象的成本，通过有效过滤机会主义主体，缩小了合作初始阶段的风险敞口，从而推动了市场交易成本显著下降，为专业化分工奠定了基础。

另一方面，在交易关系维护阶段，信息成本主要体现在沟通协调、动态协商与信任维系等方面。相较于交易关系构建阶段侧重于识别“谁值得信任”，维护阶段更强调“如何维系持续信任”。现有研究表明，数据信息泄露风险会损害供应链韧性（Kashmiri 等，2017）。耿勇等（2024）的研究也表明，一旦合作方感知到高信息风险敞口，通常会主动收缩合作规模，进而加剧原有协作关系的脆弱性。此外，信息风险还可能通过溢出效应影响整个市场。梁平汉和江鸿泽（2020）指出，网络传销事件破坏了区域的商业信誉体系，影响市场主体的合作预期。董天一等（2024）则发现，网络水军活动会显著干扰投资者的风险判断与预期理性，造成更广泛的市场行为扭曲。这些研究揭示了互联网信息风险如何通过破坏市场信任机制，抑制企业分工深化。

为应对此类信息风险，地方政府在交易维护阶段主要通过两条路径开展治理：一是针对技术性信息风险（如数据泄露、网络攻击、网络交易欺诈等），建立网络安全监管机制与风险预警平台，提升企业间数据传输的安全性与可控性；二是针对非技术性信息风险（如网络谣言、流量造假等），强化实时监测与内容治理，压缩虚假信息的传播范围与存续周期，从而维护市场主体声誉与合作信任基础。上述举措不仅显著降低了企业在交易关系维护中的沟通成本与信任修复成本，更通过稳定市场预期，引导企业将有限资源从风险应对转向分工网络拓展，推动企业专业化分工持续升级。据此，本文提出假说 1a：地方政府互联网信息风险治理能通过降低企业的市场交易成本，提升其专业化分工水平。

（二）内部管控成本主导型作用路径

当地方政府互联网信息风险治理对企业管控成本的降低幅度大于对市场交易成本的降低幅度时，企业倾向于通过纵向整合来替代市场交易。该路径可以通过信息安全维护成本与信息协调成本这两类内部管控成本的协同下降实现。

一方面，地方政府互联网信息风险治理有助于降低企业的信息安全维护支出，为其扩展纵向边界提供保障。这类成本通常源于企业为应对系统漏洞、员工误操作以及管理流程失效等信息风险所产生的制度与技术投入需求。在高度数字化环境下，病毒攻击或数据泄露等事件可能导致企业核心流程中断，进而推高信息系统加固、运维升级与应急响应成本（张文文和景维民，2024）。为此，地方政府通过建设区域信息风险监测平台、提供统一的风险数据库与安全标准，协助企业整合原本分散于法务、IT、合规等部门的风险管理资源，构建统一高效的信息安全体系；同时，通过财政补贴、标准引导和技术推广，支持企业引入智能风控工具，降低边际投入成本。借助政府提供的标准化风险数据库，企业可部分替代传统多层级内部监督机制，降低防控体系构建成本，从而增强纵向整合动力。

另一方面，地方政府互联网信息风险治理通过降低企业的信息协调成本，提升其组织运转效率，从而强化内部整合激励（Grossman 和 Hart，1986）。信息协调成本主要指企业在内部多业务单元间信息传递、流程对接与战略联动中的风险防控支出，这类成本大多源于部门间标准不统一、接口不兼容、权限混乱等问题引发的沟通障碍与决策迟滞。地方政府通过发布统一的数据分类分级规范、建立政企协同风险治理平台、引导部门数据接口标准化等方式，强化企业内部信息互通安全机制。此外，政府通过构建跨部门联合治理架构，统一监管规则，缓解多头监管带来的摩擦（申志轩等，2025），以减少企业因制度碎片化而产生的重复投入与管理失效。随着组织内部信息协同效率的提升，企业整体运营更加高效有序，纵向整合的管理基础进一步夯实。据此，本文提出假说 1b：地方政府互联网信息风险治理能通过降低企业的内部管控成本，提升其纵向一体化水平。

三、研究设计

（一）样本选择与数据来源

本文以 2011—2022 年 A 股上市公司作为初始研究样本，并对样本进行如下处理：（1）剔除金融类公司样本；（2）剔除关键变量缺失以及总资产小于 0、资产负债率大于 1 等数据异常的样本；（3）剔除 ST、*ST、PT 等被特殊处理的样本；（4）剔除企业专业化分工水平偏离合理值域 [0，1] 的样本；（5）对连续变量进行上下 1% 的缩尾处理，以减少极端值的影响。本文最终得到 24 565 个公司—年度观测值。地方政府互联网信息风险治理水平数据通过手工搜集得到，财务数据来自国泰安数据库（CSMAR）和中国研究数据服务平台（CNRDS）。

(二)地方政府互联网信息风险治理水平指标构建

1. 政策背景与概念界定。2011 年 5 月,国家互联网信息办公室成立,标志着互联网管理和决策核心机制的建立。2014 年 2 月,中央网络安全和信息化领导小组成立,推动了舆情管控、网络安全监测与信息化建设"三位一体"治理格局的形成(黎慈,2021)。此后,各地级市相继设立互联网信息办公室,构建起自上而下的政策执行体系(严兵,2022)。2017 年出台的《党委(党组)网络安全工作责任制实施办法》明确了各级党委(党组)为本地区、本部门网络安全工作的责任主体。同年,国家网信办发布《互联网信息内容管理行政执法程序规定》,将市(地、州)级网信部门确立为属地监管执法主体。这些制度安排表明,中国网络信息安全监管体系不断完善,逐步构建起以中央为核心、覆盖全国的三级网信工作体系。本文以地级市政府为责任主体,构建区域层面的互联网信息风险治理水平指标体系。地方政府互联网信息风险治理是指政府运用综合治理举措(如政策制定、监管机构设立、资金支持、行业自律、教育和宣传、专项行动开展等),实现企业、行业协会、网民等多方协同共治,以应对互联网环境中信息生成、储存、传播过程中的潜在威胁,最终提高各类信息决策应用的价值。

2. 指标构建方法

(1)互联网信息风险类型分类逻辑。本文在界定企业面临的主要互联网信息风险类型时,系统整合政策框架、企业实践与学术研究三方面依据,聚焦于与企业经营决策高度相关的三类核心风险:数据信息安全风险、平台内容传输风险和网络交易欺诈风险。这三类风险既涵盖企业数字化运营中的关键环节,也呈现出技术、社会与经济维度的系统关联,构成企业在数字环境中需重点防范的信息风险结构。三类风险定义如下:①数据信息安全风险是指网络系统漏洞、信息基础设施脆弱性或外部攻击等因素导致企业数据的保密性、完整性与可用性受到威胁的风险,涵盖网络攻击、系统入侵、数据泄露、权限滥用等。②平台内容传输风险是指互联网平台上虚假、有害、侵权或操控性内容传播所引发的信息污染、舆情冲击等导致企业声誉受损,从而干扰企业正常运行的风险,包括虚假宣传、舆论操控、流量造假、内容违规等。③网络交易欺诈风险是指企业在参与网络交易过程中因虚假信息、身份冒用、网络诈骗等因素而导致的资产损失与法律风险等。三类风险的分类逻辑如下:

首先,政策框架。国家通过"三法一条例"(即《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》)构建了涵盖数据采集、存储、使用与传输的风险治理体系,体现出对数据信息安全风险的技术性防控思路;《网络信息内容生态治理规定》压实互联网平台审核责任,强化了对平台内容传播风险的社会治理属性;《网络交易监督管理办法》《中华人民共和国反电信网络诈骗法》通过"穿透式"交易审查机制,构建起针对交易型信息风险的经济性防线。三类风险分别对应技术防控、社会治理与经济监管三类制度路径,构成了当前政策框架下的信息风险分类锚点。

其次,企业决策实践。三类风险已对企业经营活动构成实质冲击,成为影响企业运营的重要外部变量。IBM 发布的《2023 年数据泄露成本报告》显示,全球企业因单次数据泄露事件而造成的平均损失高达 445 万美元,约 60% 的企业出现客户流失,纳斯达克上市公司股价平均下跌 5%。国家网信办数据显示,2022 年约谈网站平台 8 608 家、下架违规 App 420 款,涉企网络侵权举报量占比超 30%,反映出平台内容生态失控对企业声誉的实质损害。公安部通报称,网络交易欺诈涉案金额从 2021 年的 110 亿元激增至 2024 年的 1 200 亿元,其中三成涉及企业账户洗钱。三类风险在发生频率、损失规模与影响范围上已成为企业风险图谱中的高频与高损类事件,亟须制度性治理应对。

最后，学术文献支撑。数据信息安全风险反映了企业技术系统的脆弱性（陈思翀和汪琪，2021；Eisenbach 等，2022）；平台内容传输风险体现了社会信任失灵与声誉管理困境（董天一等，2024）；网络交易欺诈风险则揭示了数字化交易环境对企业资金运作安全的潜在威胁（梁平汉和江鸿泽，2020）。从影响逻辑来看，三类风险分别嵌入企业的技术基础、社会关系与经济交易，构成了企业应对信息风险的核心治理维度。

（2）关键词选取依据。[①]在“互联网信息风险”关键词选取方面，本文采用“政策文本归纳+专业词典扩展+高频词提取”三重路径，以确保风险维度覆盖全面且关键词具有现实关联性与理论依据。首先，采集中央及地方政府发布的互联网信息风险治理相关政策法规、监管通报与典型新闻报道，通过人工标注与自动分词技术来识别与互联网信息风险相关的高频词项；其次，参考《网络空间治理词典》《公共安全治理蓝皮书》等权威工具书及相关代表性研究（范柏乃和盛中华，2024；耿勇等，2024），对词表进行语义扩展与同义词补充；最后，结合本文构建的风险分类框架，即从技术性、社会性与经济性三个维度界定的数据信息安全风险、平台内容传输风险与网络交易欺诈风险三类风险，进一步筛选能准确反映企业面临的主要互联网信息风险的关键词，确保各类风险具有理论代表性与实践辨识度。

在“治理”关键词选取方面，本文借鉴危机管理与互联网生态治理研究中的分阶段逻辑（艾祖鹏等，2023；严炜炜等，2024），将治理过程划分为预防性治理、即时性治理与结果性治理三类，分别对应风险发生前、中、后的政府角色，并据此构建地方政府互联网信息风险治理水平的一级指标体系。

（3）治理信息的提炼方式。在获取地方政府互联网信息风险治理文本数据时，本文将互联网信息风险相关关键词与全国地级及以上城市名称、治理类词汇进行组合，在政府官网及微软 Bing 平台上按年度进行检索。例如，构造“上海市+打击+黑客攻击”等词组，以捕捉各地治理实践与政策执行信息。实际操作中，检索路径存在三类噪音干扰：一是部分结果为政策解读、讲话稿或目录类内容，缺乏实质性治理信息。二是新闻报道受地方宣传能力影响，可能导致治理水平存在系统性偏误。为此，本文剔除纯宣传性内容，仅保留涉及治理行为、执行过程或绩效评估的信息，并借助文本挖掘算法排除带有明显正面修饰的无效文本。三是由于关键词组合搜索易产生重复记录，本文通过人工核读，确保所用文本确实反映治理行为，避免重复计量。最终样本涵盖各地发布的法律、法规、制度、行业指引、专项行动方案以及具有执行内容的新闻报道，构建了较为全面的治理信息数据库。

（4）指标构建。在构建地方政府互联网信息风险治理水平指标体系时，本文将其划分为预防性治理、即时性治理与结果性治理三个一级指标，并结合三类风险在政策治理中的具体表现路径，进一步细化为六个可观测、可区分的二级指标。最后，本文采用熵值法对各指标进行赋权与综合测算，[②]如图 1 和表 1 所示。一级指标和二级指标的具体构建逻辑如下：

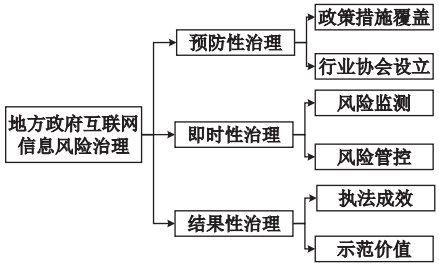

图 1　地方政府互联网信息风险治理指标体系

① 受篇幅限制，关键词词汇及定义详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

② 熵值法的计算方法详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

表 1　地方政府互联网信息风险治理指标体系

一级指标	二级指标	含义
预防性治理	政策措施覆盖	衡量地方政府在政策层面对数据信息安全、平台内容传输与网络交易欺诈三类风险的治理覆盖广度。若政策同时涵盖三类风险，则赋值为3；涵盖两类则为2；涵盖一类则为1；其他为0
	行业协会设立	评估地方政府是否设立针对三类风险的防范类行业组织，如数据安全协会、自媒体内容治理联盟和反诈联盟等。若三类均设立，则赋值为3；设立两类则为2；设立一类则为1；其他为0
即时性治理	风险监测能力	衡量地方政府是否建立相关监测机制，以实现对三类风险的实时识别，如数据信息安全监测中心、平台内容监测中心、反网络交易诈骗监测中心等。若三类监测中心均已设立，则赋值为3；设立两类则为2；设立一类则为1；均未设立则为0
	风险管控能力	反映地方政府对互联网信息风险事件的干预频率与应急能力，采用政府开展网络安全检查、内容清理、反诈整治等行动的频次加1后取自然对数
结果性治理	执法成效	衡量地方政府打击互联网信息风险类违法犯罪的成效，统计数据信息侵犯、平台内容违法与网络交易欺诈三类案件的破案总数加1后取自然对数
	示范价值	评估地方政府治理行动的引领性与外溢价值。若地方政府在互联网信息风险治理中作出突出贡献（如成立示范区、获奖表彰等），则赋值为1，否则为0

预防性治理侧重从事前控制角度评估政府是否在信息风险显性化之前通过制定规范、建立机制、设立组织等方式提前介入，体现了治理的规则先行与前置控制属性。三类互联网信息风险本质上对制度供给提出了差异化治理需求，在此维度下本文设置两个二级指标：一是政策措施覆盖，旨在衡量地方政府是否在数据信息、平台内容与网络交易等核心领域出台全面的政策或治理机制，这是实现三类风险制度化管理的基础；二是行业协会设立，侧重于评估地方政府是否推动成立数据安全协会、自媒体内容治理联盟或反通信网络诈骗联盟等专业组织，反映政府在应对三类风险时的前端治理与协同防控能力。

即时性治理侧重从事中监管角度评估地方政府在信息风险发生或扩散过程中是否具备快速感知、及时响应与动态处置的能力。该阶段对应三类风险在技术识别与应急响应方面的可控性要求，本文设置两个二级指标：一是风险监测能力，考察是否设有数据信息交互风险监测、舆情内容感知、网络交易风险智能监控等系统，体现地方政府对三类风险进行实时识别和动态追踪的能力；二是风险管控能力，以政府开展网络安全检查、内容清理、反诈协同整治等应急行动的频次为依据，衡量其对不同类型风险事件的快速处置与应急调控能力。

结果性治理侧重从事后处置角度评估政府治理举措是否实现了明确的治理成效，并具有可复制、可推广的示范价值。该阶段反映三类风险治理的最终绩效表现及社会反馈，本文设置两个二级指标：一是执法成效，用以量化地方政府在打击网络攻击、治理有害信息、查处非法交易等方面的实际成效，反映治理措施在执法层面的落地情况；二是示范价值，聚焦治理模式是否被认定为典型案例或纳入治理试点，以体现三类风险治理经验的可推广性与制度外溢能力。

（三）模型设定

本文构建模型（1）来考察地方政府互联网信息风险治理对企业专业化分工水平的影响。

$$VSI_{i,t}=\beta_0+\beta_1 WebGov_{m,t}+\gamma Controls_{im,t}+\sum Firm+\sum City+\sum Year+\varepsilon_{i,t} \quad (1)$$

其中，解释变量$WebGov_{m,t}$为地级市互联网信息风险治理水平，被解释变量$VSI_{i,t}$为价值增值法度量的企业专业化分工水平。[①]参考现有文献（赵云辉等，2019；袁淳等，2023）的做法，控制变量$Controls_{im,t}$包括企业层面与地区层面的其他影响因素。同时，本文控制了公司、地区和年度固定效应。$\varepsilon_{i,t}$为随机扰动项。本文主要变量定义与描述性统计结果见表 2。[②]

① 企业专业化分工水平的计算方式详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

② 受篇幅限制，主要变量定义及计算方式详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

表 2　主要变量定义与描述性统计

变量符号	变量名称	观测数	均值	标准差	最小值	最大值
VSI	企业专业化分工	24 565	0.5606	0.2112	0.0500	0.9634
WebGov	地方政府互联网信息风险治理	24 565	20.4281	18.0988	0.0005	74.2018
Size	企业规模	24 565	22.3415	1.3221	19.8104	26.4129
Lev	资产负债率	24 565	0.4483	0.1970	0.0619	0.8877
Age	企业年龄	24 565	2.1670	0.7876	0.0000	3.3322
Cap	资本密集度	24 565	2.2384	1.4876	0.4121	9.1406
Roa	总资产净利润率	24 565	0.0341	0.0568	−0.2228	0.1803
MB	账面市值比	24 565	0.6386	0.2462	0.1285	1.1851
SOE	产权性质	24 565	0.3553	0.4786	0.0000	1.0000
Balance	股权制衡度	24 565	0.7240	0.5948	0.0280	2.6995
Subs	子公司数量	24 565	2.7960	1.0063	0.0000	5.3375
Inform	地区数字经济发展水平	24 565	1.0869	1.1165	−1.2632	3.8392
GDP	地区经济发展水平	24 565	11.4033	0.5151	9.9271	12.4542
Service	政府公共服务能力	24 565	0.0919	0.0197	0.0425	0.1326
Crime	政府法治建设	24 565	0.0606	0.0311	0.0133	0.1726
Regul	地区监管质量	24 565	1.2941	0.1199	1.0310	1.6718

四、实证分析

（一）描述性统计

本文对全国地级市互联网信息风险治理指标进行了时间与空间维度的分析。结果显示，2011—2022 年全国地级市的互联网信息风险治理水平整体呈稳步上升态势，反映出治理能力持续增强。其中，2016 年该指标出现显著跃升，这主要得益于当年国家在网络安全领域制度建设的密集推进，包括《中华人民共和国网络安全法》的正式颁布，以及中国网络空间安全协会的成立、《国家信息化发展战略纲要》《国家网络空间安全战略》等关键文件的发布，这标志着互联网信息风险治理进入制度化、系统化阶段。类似地，2021 年该指标明显上升，对应《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络交易监督管理办法》《关于进一步压实网站平台信息内容管理主体责任的意见》等法律法规的集中出台。这强化了政府在数据信息流通、互联网平台内容、网络交易等领域的监管力度，推动了地方治理水平进一步提升。总体而言，上述分析结果所反映的时间演变趋势与国家政策节奏高度契合，从侧面印证了本文构建的治理指标具有良好的现实基础与解释力。

本文进一步考察了地区互联网信息风险治理指标在空间分布上的特征。整体来看，治理水平较高的地区主要集中于东部沿海省份与核心城市，呈现以区域中心城市为核心、向周边辐射的“梯度扩展”格局。这一现象在空间维度上验证了该指标体系在刻画地区治理差异方面的有效性与现实合理性。然而，这一现象也提示了潜在的内生性问题，即治理水平较高的地区往往本身数字经济基础较好、政府治理能力较强，可能天然地更有利于企业专业化分工的深化。因此，治理水平与企业分工之间的关系可能部分源于共同的区域发展基础。为缓解这一内生性干扰，本文在实证分析中引入了地区数字化发展水平、政府治理能力等关键控制变量，并纳入公司、地区以及年度固定效应；同时，采用工具变量法、双重差分法以及多项稳健性检验，以增强因果识别的可信度与实证结果的稳健性。

（二）基准回归[①]

表 3 汇报了地方政府互联网信息风险治理水平对企业专业化分工影响的基准回归结果。[②]列（1）和列（2）分别展示了仅控制公司、地区与年度固定效应，以及在此基础上纳入公司与地区层面控制变量后的估计结果。核心解释变量 *WebGov* 的回归系数均在 1% 的水平上显著为正，验证了假说 1a，即地方政府互联网信息风险治理水平的提升显著促进了企业专业化分工。导致这一结果的原因可能在于，相较于政府通过互联网信息风险治理优化市场交易环境、稳定市场预期所带来的直接激励，企业内部管控成本的改善路径更加复杂，其优化效果更依赖于企业是否具备围绕信息风险治理进行技术架构重构、组织流程再造与人员配置优化的能力，本质上是一种高度嵌入、系统性的组织变革（范柏乃和盛中华，2024）。一方面，企业可能因组织惰性和路径依赖而对政策激励反应迟缓（吕一博等，2015）；另一方面，内部治理体系建设往往面临跨部门协调困难，导致改革阻力与成本增加（易加斌等，2022）。因此，当前阶段地方政府的互联网信息风险治理主要通过降低市场交易成本来激发企业专业化分工的积极性，而在降低企业内部管控成本方面的作用仍受到一定的结构性约束。

表 3　基准回归

	（1） *VSI*	（2） *VSI*
WebGov	0.0327***	0.0282***
	（2.989）	（2.731）
Controls	未控制	控制
Firm、*City*和*Year*	控制	控制
N	24 565	24 565
Adj. R^2	0.607	0.626

注：括号内为聚类到行业—年度层面的稳健*t*值，*、**和***分别表示在10%、5%和1%水平上显著。下表同。

（三）内生性检验

一方面，无法观测的时间趋势和地区特征可能同时推动地方政府互联网信息风险治理水平与企业专业化分工水平的上升，导致结果偏误；另一方面，可能存在反向因果问题，即企业专业化分工水平提升可能促使政府加强互联网信息风险治理。为缓解上述内生性问题，本文采用双重差分法、安慰剂检验和工具变量法对两者关系进行重新识别。

1. 双重差分检验。2017 年底，工业和信息化部与北京市签署协议共建国家网络安全产业园区，标志着我国互联网安全治理迈入产业化、系统化阶段。在此前后，杭州、成都、三亚、南京等地相继设立本地网络安全产业园，这些园区在地方政府推动下引入信息安全企业，建设集监测预警、漏洞修复、运行防护等功能于一体的综合平台，向企业提供网站防护、DDoS 检测、APT 识别、诈骗监测等多样化服务。园区提升了地方政府对区域互联网信息风险的协同预警与快速响应能力，显著增强了当地互联网信息风险治理水平。作为具有政策推动特征的外部冲击，网络安全产业园的落地具有较强的外生性。据此，本文构建双重差分模型（2），检验网络安全产业园建立对企业专业化分工水平的影响。

$$VSI_{i,t}=\beta_0+\beta_1 Treat_i\times Post_t+\gamma Controls_{im,t}+\sum Firm+\sum City+\sum Year+\varepsilon_{i,t} \quad (2)$$

其中，$Treat_i$ 为处理组虚拟变量，若地级市在样本期间设立了网络安全产业园，则取值为 1，否则为 0。$Post_t$ 为时间虚拟变量，若年份处于该市设立网络安全产业园当年及之后，则取值为 1，否则为 0。其他控制变量与模型（1）一致。为缓解样本选择偏误，本文基于控制变量构建 Probit 模型计算倾向得分，采用 1∶1 最近邻匹配法（卡尺设定为 0.02），选取得分最接近的对照组样本，并对匹配后的样本进行双重差分估计。

① 受篇幅限制，基准回归分析的完整结果详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

② 为提高回归系数的可读性，本文在回归时将变量 *WebGov* 缩小了 100 倍。

表 4 结果显示，[①]无论是采用 DID 模型还是 PSM-DID 模型，交互项 *Treat*×*Post* 的系数均显著为正。这表明，相较于未建立网络安全产业园的地区，设立网络安全产业园能够显著提升当地互联网信息风险治理成效，进而促进企业专业化分工。此外，该结果通过了平行趋势检验，[②]进一步验证了基准回归结论的稳健性。

表 4　双重差分检验

	（1） DID	（2） PSM-DID
	VSI	*VSI*
Treat×*Post*	0.0145***	0.0105*
	（2.901）	（1.949）
Controls	控制	控制
Firm、*City*和*Year*	控制	控制
N	24 565	13 939
Adj. R^2	0.626	0.628

2. 安慰剂检验。[③]本文通过随机生成伪处理组，替换模型（2）中的 *Treat* 进行回归，并重复该过程 500 次，绘制 *Treat*×*Post* 估计系数的核密度图。结果显示，随机估计系数的均值接近 0，*p* 值大多大于 0.1，且伪处理组所得系数与 *Treat*×*Post* 的实际估计值（0.0145）显著不同。这表明在缓解解释变量测量误差后，结果依然保持稳健。

3. 工具变量检验。[④]借鉴张文文和景维民（2024）的研究，本文采用与互联网信息风险治理相关的行政处罚数据构造工具变量，分别为地级市公共安全类处罚事件的自然对数与地级市土地城建类处罚事件的自然对数。一方面，这两类处罚数据在一定程度上能够体现地区执法监管习惯及治理力度，与互联网信息风险治理水平具有相关性；另一方面，这两类处罚分别涉及城市治安和城市建设，与企业专业化分工水平无直接关联，具有一定的外生性。在排除弱工具变量假设的前提下，*WebGov* 的回归系数显著为正，这进一步增强了基准回归结果的稳健性。

（四）其他稳健性检验[⑤]

为增强实证结果的稳健性，本文采用多种方法进行检验。（1）筛选样本：剔除企业注册地位于北京、上海、天津、重庆、广州、深圳、杭州、宁波、南京、福州、厦门、海口等治理能力较强、企业资源禀赋较高地区的样本，以控制其系统性偏高的专业化分工水平，在此基础上重新进行回归。（2）替换变量：一是采用主成分分析法重构互联网信息风险治理水平指标；二是更换采购商品增值税税率与净资产指标，重新测算企业专业化分工水平。（3）调整模型：将模型聚类到城市—年度层面进行估计。（4）控制异地子公司：考虑到异地子公司所在地互联网信息风险治理对企业分工决策的影响，控制异地子公司数量占比后重新进行回归。上述检验结果均未改变本文的核心结论。

五、进一步研究

（一）机制检验

本文进一步探讨地方政府互联网信息风险治理如何通过影响企业在交易关系构建与维护阶段的信息成本，促进企业专业化分工。借鉴江艇（2022）运用调节效应识别因果机制的思路，若市场交易成本是关键传导路径，则在交易成本较高的情境下，互联网信息风险治理的效应会更加显著。为系统检验该机制，本文从企业与地区两个层面分别展开分析。

① 受篇幅限制，双重差分检验的完整结果详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

② 受篇幅限制，平行趋势检验结果详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

③ 受篇幅限制，安慰剂检验结果详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

④ 受篇幅限制，工具变量检验结果详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

⑤ 受篇幅限制，其他稳健性检验结果详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

1. 企业层面信息成本。本文以企业资产专用性和供需偏离度作为微观层面的调节变量。一方面，资产专用性较高的企业对特定交易关系的依赖较强，在构建交易关系时需投入更多资源筛选信息，以降低合作中断风险（Williamson，1985）；另一方面，供需偏离度较高的企业因生产计划与市场需求错配，交易维护过程中更易面临频繁的契约再谈判，进而抬升信息成本（李青原等，2023）。借鉴郝闻汉等（2021）的研究，本文使用退出价值来度量企业资产专用性（*Exit*），若其高于年度行业中位数，则 *Exit* 取值为 1，否则为 0；参考杨志强等（2020）的研究，以供应商企业与其客户企业的供需偏离度之比来衡量企业供应链中的“牛鞭效应”（*FSD*），若其高于年度行业中位数，则 *FSD* 取值为 1，否则为 0。表 5 结果显示，*WebGov*×*Exit* 和 *WebGov*×*FSD* 的系数均显著为正，表明在资产专用性或供需偏离度较高的情境下，地方政府互联网信息风险治理对企业专业化分工的促进作用更加显著。上述结果表明，地方政府互联网信息风险治理通过有效降低微观层面的信息成本，促进企业专业化分工。

表 5　机制检验：企业层面信息成本

	（1） 资产专用性	（2） 供需偏离度
	VSI	*VSI*
WebGov×*Exit*	0.0334**	
	（2.297）	
WebGov×*FSD*		0.0217**
		（2.113）
WebGov	0.0164	0.0209*
	（1.380）	（1.938）
Exit	−0.0170***	
	（−3.278）	
FSD		0.0010
		（0.333）
Controls	控制	控制
Firm、*City*和*Year*	控制	控制
N	24 565	24 565
Adj. R^2	0.626	0.626

表 6　机制检验：地区层面信息成本

	（1） 线上交易活跃度	（2） 商业信用环境
	VSI	*VSI*
WebGov×*ElecFirm*	−0.0904***	
	（−5.004）	
WebGov×*CityTrust*		−0.0436***
		（−2.672）
WebGov	0.0888***	0.0574***
	（4.995）	（3.745）
ElecFirm	0.0087**	
	（1.973）	
CityTrust		0.0067
		（1.470）
Controls	控制	控制
Firm、*City*和*Year*	控制	控制
N	24 565	24 565
Adj. R^2	0.627	0.627

2. 地区层面信息成本。本文以地区交易活跃度与城市商业信用环境指数来衡量宏观层面的信息成本。一方面，在交易活跃度较低的地区，平台型市场主体供给不足、信息交互效率较低，企业在交易关系的建立与维系过程中面临更高的信息成本；另一方面，城市商业信用环境较差的地区存在信任缺失，企业不仅需要在交易关系构建阶段承担更高的信息成本用于识别可靠的交易对象，同时在交易维护阶段也需支付更高的信任修复成本，以应对潜在的信息交互风险。本文以电子商务交易活跃度来表征企业线上交易活跃度（*ElecFirm*），若其高于年度中位数，则 *ElecFirm* 取值为 1，否则为 0。参考李文钊等（2023）的研究，本文使用中国城市商业信用环境指数来度量地区商业信用质量（*CityTrust*），若其高于年度中位数，则 *CityTrust* 取值为 1，否则为 0。该指数涵盖信用工具、征信体系、失信行为等维度，较为全面地反映了城市信用状况。表 6 结果显示，*WebGov*×*ElecFirm* 和 *WebGov*×*CityTrust* 的系数均显著为负，表明在线上交易活跃度较低、商业信用环境较差的情况下，地方政府互联网信息风险治理对企业专业化分工的促进作用更加显著。上述结果表明，地方政府互联网信息风险治理通过降低宏观层面的信息成本，推动企业分工深化。

（二）异质性分析[①]

上文机制分析表明，地方政府互联网信息风险治理通过降低企业在交易关系构建与维护阶段的信息成本，促进企业专业化分工。而企业专业化分工决策不仅受信息成本影响，还受地区治理特征与企业行业特性的影响。因此，本文从这两个方面展开异质性分析。

1. 基于地区治理特征的异质性分析。互联网信息风险治理涉及政府对企业、行业协会、网民等多主体的协调能力，对不同治理工具的使用效率以及治理执行力。为此，本文主要从治理主体协同性、治理效率以及治理执行力三个维度，构建地方政府互联网信息风险治理的差异化特征分析框架。（1）治理主体协同性：衡量地方政府是否实现多元主体协同共治。若某地级市当年通过政策、治理实践或舆情资料体现企业、行业协会或网民等非政府主体参与，则具备治理多样性。典型案例包括：山东省建立网络安全重点企业（机构）库，引导重点企业在技术创新、人才培养、产业发展中发挥网络安全建设方面的示范带动作用；在行业协会参与治理方面，连云港设立网络空间安全学会推动行业自律；南京组建网络生态治理志愿者团队，引导公众参与网络秩序维护。（2）治理效率：衡量地方政府是否有效利用信息技术来提升风险识别与响应效率。若当年地方政府在治理实践中借助信息风险监测平台等技术工具进行风险识别、预警或打击网络违法行为，则治理效率较高。典型案例包括：上海市打造 AI 全链条反诈体系；吉林市场监管部门开发网络交易监测系统。（3）治理执行力：衡量地方政府在互联网信息风险治理中是否具备较强的政策执行能力，能将政策文件转化为具体治理行动。重点关注是否公开违法行为惩戒措施或案件查处情况，若披露对违法主体的处罚信息（如罚款、拘留等），则认为其治理执行力较强。典型案例包括：对网络“刷单”企业实施行政处罚、对编造传播网络谣言的个人实施治安拘留等实质性执法行动。异质性分析结果显示，调动多主体参与治理、提高治理效率以及增强治理执行力均有助于增强地方政府互联网信息风险治理对企业专业化分工的积极作用。

2. 基于企业行业特征的异质性分析。鉴于不同行业在市场环境和信息依赖度方面的差异，本文探讨了地方政府互联网信息风险治理对企业专业化分工的行业异质性影响。（1）市场环境：采用同年同行业各企业营业收入所占市场份额计算赫芬达尔指数，用以衡量行业竞争度。结果显示，在竞争较为激烈的行业中，企业因缺乏足够资源和能力应对信息风险，地方政府互联网信息风险治理对企业专业化分工的促进作用更加显著。（2）信息依赖度：区分企业是否为现代服务业企业。现代服务业通常信息密集度较高，其服务交付、客户关系管理和运营管理均依赖于大量的信息处理与传递，易遭受互联网信息风险冲击。结果显示，互联网信息风险治理能够显著提升现代服务业的信息传递可靠性与效率，从而促进该行业的专业化分工。

六、结论与启示

专业化分工不仅是企业强化核心竞争力的关键路径，也是当前提升供给质量与效率的重要手段。随着数字技术与实体经济的深度融合，企业分工日趋平台化、智能化，同时也面临信息风险带来的新型市场不确定性。为应对这一挑战，本文从预防性治理、即时性治理和结果性治理三个维度出发，构建了地方政府互联网信息风险治理水平指标体系，并从信息成本视角系统分析了其对企业专业化分工的影响机制。研究发现，地方政府信息风险治理水平的提升显著促进了企业专业化分工，这主要通过降低企业在交易关系构建与维护阶段的信息成本而实现。异质性分析发现，多元主体协同、技术赋能提升治理效率、强化执行力均有助于增强治理效应；此

① 受篇幅限制，异质性分析检验结果详见《财经研究》网站（https://qks.sufe.edu.cn/J/CJYJ.html/CN）文章附件。

外，在竞争较为激烈或信息依赖度较高的行业中，治理的边际效应更加突出。本文的研究具有以下政策启示：

对政府部门而言，首先应从预防性、即时性、结果性等多个维度，系统评估地方政府互联网信息安全建设情况，压实地方政府治理责任。本文发现，地方政府多以事后惩戒或运动式治理为主，防范制度相对薄弱，不利于从源头控制企业所面临的各类信息风险。因此，应加强事前预防和事中控制，并执行统一的风险管理标准，为企业开展专业化分工提供“算法信任”。其次，鉴于不同行业企业的信息风险敞口和应对能力存在差异，政府应避免采取“一刀切”的监管方式。应通过调研、问卷、线上评估等手段，对企业风险进行分级分类，提供差异化的信息安全资金补贴与技术支持。最后，应鼓励多元主体参与信息风险治理，推动建立协调顺畅、合作高效的政府监管体系。政府应通过招商引资、税收优惠、战略合作等方式，引导社会资本参与信息安全产业建设；同时，加强网络安全宣传，完善举报机制，构建高效协同的网络安全治理格局。

对企业管理者而言，在开展专业化分工时，应关注地方政府在互联网信息生态建设方面的能力，包括是否提供信息安全培训与技术支持、是否设有网络交易监管平台以及自媒体治理力度大小等。尤其是网络风险敞口大、应对能力弱的企业，更应优先选择互联网信息风险治理水平较高的地区作为经营地。此外，企业在优化专业化分工的过程中，应注重市场交易前、合约缔结过程中以及交易达成后全过程的信息成本管理，并结合业务特征识别核心信息风险，合理配置治理资源。例如，对于依赖大量数据处理的企业，应优先投入数据加密与安全防护技术；对于依赖用户口碑和信任的企业，应配置舆情公关人员和平台内容监测机制；对于涉及网络交易的平台型企业，可设立首席技术官岗位，以保障交易安全。

参考文献：

[1]艾祖鹏，梁蕴泽，郭文强. 中国互联网信息内容生态治理策略体系构建与演化研究[A]. 第十八届（2023）中国管理学年会暨“一带一路”十周年研讨会论文集[C]. 乌鲁木齐：中国管理现代化研究会，复旦管理学奖励基金会，2023.

[2]陈思翀，汪琪. 网络安全事件披露的市场冲击及行业扩散效应[J]. 经济与管理研究，2021，（6）：65−79.

[3]董天一，鲁桂华，王玉涛. 网络水军与资源配置效率：基于大股东减持视角[J]. 南开管理评论，2024，（6）：160−171.

[4]范柏乃，盛中华. 数字风险治理：研究脉络、理论框架及未来展望[J]. 管理世界，2024，（8）：208−235，12.

[5]耿勇，向晓建，万攀兵. 供应链信任衰退：网络安全风险与企业贸易信贷[J]. 中国工业经济，2024，（5）：135−154.

[6]郝闻汉，袁淳，耿春晓. 区域一体化政策能促进企业垂直分工吗？——来自撤县设区的证据[J]. 经济管理，2021，（6）：22−37.

[7]江艇. 因果推断经验研究中的中介效应与调节效应[J]. 中国工业经济，2022，（5）：100−120.

[8]黎慈. 共治网络：网络社会治理的政策工具分析[D]. 武汉：华中师范大学，2021.

[9]李青原，李昱，章尹赛楠，等. 企业数字化转型的信息溢出效应——基于供应链视角的经验证据[J]. 中国工业经济，2023，（7）：142−159.

[10]李文钊，翟文康，刘文璋. “放管服”改革何以优化营商环境？——基于治理结构视角[J]. 管理世界，2023，（9）：104−123.

[11]梁平汉，江鸿泽. 金融可得性与互联网金融风险防范——基于网络传销案件的实证分析[J]. 中国工业经济，2020，（4）：116−134.

[12]吕一博，程露，苏敬勤. 组织惯性对集群网络演化的影响研究——基于多主体建模的仿真分析[J]. 管理科学学报，2015，（6）：30−40.

[13]沈坤荣，林剑威，傅元海. 网络基础设施建设、信息可得性与企业创新边界[J]. 中国工业经济，2023，(1)：57−75.

[14]申志轩，祝树金，文茜，等. 以有为政府赋能有效市场：政府数字治理与企业投资效率[J]. 世界经济，2025，(2)：166−195.

[15]施炳展，李建桐. 互联网是否促进了分工：来自中国制造业企业的证据[J]. 管理世界，2020，(4)：130−148.

[16]严兵. 中国网络内容治理政策的演变与未来选择[D]. 重庆：西南政法大学，2022.

[17]严炜炜，宋佳慧，王妍妍. 基于制度文本分析的网络信息内容生态协同治理研究[J]. 图书情报知识，2024，(5)：115−127.

[18]杨志强，唐松，李增泉. 资本市场信息披露、关系型合约与供需长鞭效应——基于供应链信息外溢的经验证据[J]. 管理世界，2020，(7)：89−105.

[19]易加斌，张梓仪，杨小平，等. 互联网企业组织惯性、数字化能力与商业模式创新[J]. 南开管理评论，2022，(5)：29−40.

[20]袁淳，从阙匀，耿春晓. 信息基础设施建设与企业专业化分工——基于国家智慧城市建设的自然实验[J]. 财经研究，2023，(6)：34−48.

[21]张文文，景维民. 数字经济监管与企业数字化转型——基于收益和成本的权衡分析[J]. 数量经济技术经济研究，2024，(1)：5−24.

[22]赵云辉，张哲，冯泰文，等. 大数据发展、制度环境与政府治理效率[J]. 管理世界，2019，(11)：119−132.

[23]甄杰，谢宗晓，李康宏，等. 信息安全治理与企业绩效：一个被调节的中介作用模型[J]. 南开管理评论，2020，(1)：158−168.

[24]Acemoglu D，Griffith R，Aghion P，et al. Vertical integration and technology：Theory and evidence[J]. Journal of the European Economic Association，2010，8(5)：989−1033.

[25]Cao S S，Fang V W，Lei L J. Negative peer disclosure[J]. Journal of Financial Economics，2021，140(3)：815−837.

[26]Coase R H. The nature of the firm[J]. Economica，1937，4(16)：386−405.

[27]Eisenbach T M，Kovner A，Lee M J. Cyber risk and the U.S. financial system：A pre-mortem analysis[J]. Journal of Financial Economics，2022，145(3)：802−826.

[28]Grossman S J，Hart O D. The costs and benefits of ownership：A theory of vertical and lateral integration[J]. Journal of Political Economy，1986，94(4)：691−719.

[29]Kashmiri S，Nicol C D，Hsu L. Birds of a feather：Intra-industry spillover of the target customer data breach and the shielding role of IT，marketing，and CSR[J]. Journal of the Academy of Marketing Science，2017，45(2)：208−228.

[30]Mizutani F，Smith A，Nash C，et al. Comparing the costs of vertical separation，integration，and intermediate organisational structures in European and East Asian railways[J]. Journal of Transport Economics and Policy，2015，49(3)：496−515.

[31]North D C. Institutions，institutional change，and economic performance[M]. Cambridge：Cambridge University，1990.

[32]Posey C，Roberts T L，Lowry P B. The impact of organizational commitment on insiders' motivation to protect organizational information assets[J]. Journal of Management Information Systems，2015，32(4)：179−214.

[33]Redman T C. Data's credibility problem[J]. Harvard Business Review，2013，91(12)：84−88.

[34]Scott W R. Financial accounting theory[M]. Upper Saddle River：Prentice Hall，1997.

[35]Walker G，Weber D. A transaction cost approach to make-or-buy decisions[J]. Administrative Science Quarterly，1984，29(3)：373−391.

[36]Williamson O E. Transaction-cost economics：The governance of contractual relations[J]. Journal of Law & Economics，1979，22(2)：233−261.

[37]Williamson O E. The economic institutions of capitalism: Firms, markets, relational contracting[M]. New York: Free Press, 1985.

Local Government Internet Information Risk Governance, Information Costs, and Enterprise Vertical Specialization

Jiang Muzi[1], Lu Dong[2], Chen Ying[2]

(1. *School of Economics and Management*, *Sichuan Open University*, *Chengdu* 610021, *China*;
2. *School of Accounting*, *Southwestern University of Finance and Economics*, *Chengdu* 611130, *China*)

Summary: With data deeply embedded in enterprise operations, Internet information risks have become externalized and systemic, severely threatening enterprise stability. In this context, enterprise vertical specialization is facing severe challenges, as data interconnectivity increases information leakage and cybersecurity conflicts, weakening long-term cooperation and causing "de-specialization". Enterprises struggle to combat cyber crime due to information silos, limited resources, and weak awareness, with some managers perceiving a conflict between pursuing performance and investing in security, resulting in insufficient market-driven information risk mitigation. The unique value of local government Internet information risk governance lies in supplying institutional public goods that enable a virtuous cycle of "controllable risks and deepened specialization", resolving the security-efficiency dilemma. However, existing research lacks a systematic framework for local government governance evaluation. Therefore, approaching from the perspective of local government Internet information risk governance provides a novel analytical dimension for addressing the weakening of vertical specialization in the digital economy.

This paper constructs an indicator system for local government Internet information risk governance based on relevant laws, cybersecurity strategies, and enforcement actions, encompassing preventive, real-time, and outcome-based dimensions. The empirical results show that improved governance significantly promotes enterprise vertical specialization by reducing information costs in both the formation and maintenance of transactional relationships. Heterogeneity analysis reveals that enhancements in coordination, efficiency, and deterrence strengthen governance effectiveness, especially in competitive industries and sectors with greater external information dependency.

The marginal contributions of this paper are threefold: First, it broadens the understanding of micro-level enterprise decisions by introducing an information risk governance perspective in the digital context. Second, it refines the transaction cost theory by distinguishing information costs in the formation and maintenance of transactional relationships. Third, it develops a governance evaluation system tailored to the digital economy, assessing local government performance across preventive, responsive, and outcome-based dimensions.

Key words: Internet information risk governance; information costs; enterprise vertical specialization

（责任编辑　康　健）