doi. 10. 3724/1005-0566. 20250713

网络安全风险管理与企业数字化转型

王正文,张青未,范　斐
(武汉大学经济与管理学院, 湖北　武汉　430072)

摘　要:近年来信息技术快速发展,数字化转型成为企业高质量发展的必由之路,然而信息红利背后网络安全威胁日益突出,实施网络安全风险管理至关重要。在此背景下,以2007—2023年中国A股上市企业为研究样本,实证考察企业实施网络安全风险管理对数字化转型的影响,并从异质性分析、渠道检验、经济后果检验3个方面进行拓展性讨论。研究发现,实施网络安全风险管理能够显著促进企业数字化转型。首次将网络安全风险管理与数字化转型纳入统一分析框架之中,不仅丰富了网络安全风险管理领域在中国情境下的研究,对于企业进一步完善网络安全风险管理、破解数字化转型困境也具有重要意义。

关键词:网络安全风险管理;数字化转型;文本分析法
中图分类号:F842. 6　　**文献标识码**:A　　**文章编号**:1005 - 0566(2025)07 - 0145 - 12

Cybersecurity risk management and enterprise digital transformation

WANG Zhengwen, ZHANG Qingwei, FAN Fei
(*School of Economics and Management*, *Wuhan University*, *Wuhan* 430072, *China*)

Abstract: Recent technological advances have positioned digital transformation as a necessary path for enterprise development, but growing cybersecurity threats make risk management imperative. This paper conducted a research on the impact of cybersecurity risk management implementation on enterprise digital transformation, by means of data from 2007—2023 of A-share listed companies in China. Extended discussions are conducted through heterogeneity analysis, mechanism test, and economics consequences verification. Results demonstrate significant positive effects, revealing that cybersecurity risk management implementation can accelerate enterprise digital transformation. These findings contribute to enriching cybersecurity risk management research in the Chinese context and providing practical insights for enterprises to enhance cybersecurity risk management and overcome digital transformation dilemmas.

Key words: cybersecurity risk management; enterprise digital transformation; text recognition

近年来,以大数据、云计算及人工智能为主导的新一代信息技术迅猛发展,人类世界迎来信息时代的新一轮红利。世界各国纷纷抢抓数字化发展机遇,将发展数字经济作为重要的国家战略。2015年,我国发布《促进大数据发展行动纲要》。在2016年举行的杭州峰会上,我国首次正式提出"数字经济"相关概念。党的二十大报告强调,要加快发展数字经济,促进数字经济和实体经济深度融合。2023年,我国发布《数字中国建设整体布局规划》,提出要培育壮大数字经济核心产业,打造具有国际竞争力的数字产业集群。2024年,习近平主席在世界互联网大会开幕时强调要把握数字化、网络化、智能化发展大势,把创新作为第一动力,把安全作为底线要求,把普惠作为价值追

收稿日期:2025-05-06　　**修回日期**:2025-07-08
基金项目:国家社会科学基金一般项目"网络安全风险管理促进企业数字化转型的机制与政策研究"(24BJY069)。
作者简介:王正文(1983—),男,湖北武汉人,武汉大学经济与管理学院副教授,博士生导师,研究方向为风险管理与保险。通信作者:范斐。

求,加快推动网络空间创新发展、安全发展、普惠发展,携手迈进更加美好的“数字未来”。同年,相关部门印发《中小企业数字化赋能专项行动方案(2025—2027 年)》《制造业企业数字化转型实施指南》等多项文件,由点及面、由表及里、系统化推进企业数字化转型。在此背景下,数字化转型已成为企业实现提质增效的必然选择,但实际上,企业在推进数字化转型过程中仍面临着诸多挑战。受限于转型能力不足、成本高昂及适应期漫长等因素,许多企业陷入转型意愿不足、能力缺失和风险规避的困境。因此,探索促进企业数字化转型的有效路径成为社会各界关注的重点议题。

国家“十四五”规划纲要指出,要营造良好数字经济生态,必须筑牢网络安全屏障。网络安全风险作为组织面临的十大风险之一[1],直接关系到企业的数字化转型过程。与传统项目的风险不同,信息系统的动态性和复杂性,使得网络安全风险呈现系统性、相依性以及高频低损与低频巨损兼具的特征。近年来,我国面临的网络安全威胁形势严峻且呈现持续增长态势。中国信息通信研究院测算显示,2023 年网络犯罪对我国数字经济造成的间接损失约占 GDP 的 0.8%,规模达万亿元人民币级别。根据国家互联网应急中心发布的数据,2023 年我国全年监测发现超过 319 万个恶意程序样本,针对关键信息基础设施的网络攻击同比上升 12.5%。而 2024 年上半年监测到针对工业控制系统的网络攻击同比激增 23%,恶意程序样本数量已达 220 万个,接近 2023 年全年的 70%。因此,实施网络安全风险管理对企业来说至关重要,这也将显著影响企业的数字化转型进程。一方面,网络安全风险管理的实施或能助推企业数字化转型,发挥积极影响。现有研究表明,企业主动实施网络安全风险管理有助于降低风险事件的发生概率[2],并提高投资者信心,从而为企业数字化转型构建安全屏障和缓解融资约束。另一方面,网络安全风险管理的落地需要企业在成本、劳动力和技术设备方面进行投资,这给企业带来了巨大的财务压力[3]。网络安全保险的承保双方在被保企业实际网络安全风险情况方面存在信息不对称,在短期内可能投入产出比较低,效果不显著,甚至会对企业数字化转型产生抑制作用。

现有文献主要聚焦于网络安全风险管理的实施策略、内外部驱动要素及其对企业的影响。然而,针对网络安全风险管理与企业数字化转型关系的研究,仍多停留于现象描述层面,缺乏系统的理论与实证支撑。且现有成果多基于欧美情境,在中国独特的制度背景下,企业实施网络安全风险管理对数字化转型将产生何种影响尚未得到充分的关注。

基于上述分析,本文借鉴已有文献思路,通过对上市公司年报的文本挖掘获取网络安全风险管理相关指标的数据。以 2007—2023 年中国 A 股上市企业为研究样本,实证考察企业实施网络安全风险管理对数字化转型的影响,并进行了异质性分析、渠道检验、经济后果检验。本文的主要创新点体现在 3 个方面:首先,聚焦于中国上市公司样本,评估实施网络安全风险管理对企业数字化转型的影响,丰富了网络安全风险管理领域在中国情境下的研究;其次,首次将网络安全风险管理与数字化转型纳入统一分析框架之中,为企业数字化转型提供了新的视角,得出实施网络安全风险管理是赋能数字化转型的重要途径,为企业重视网络安全风险管理提供了依据;最后,从推动数字专利申请、提高长期投资者持有比例、增加研发支出 3 个维度考察网络安全风险管理推动企业数字化转型的潜在影响渠道,从企业所有制、所在行业、所在地区、网络安全意识强弱等方面进行异质性分析,从短期绩效和全要素生产率两个方面进行经济后果检验。

一、文献综述与研究假设

(一)企业数字化转型研究现状

数字化转型是指将传统生产模式与数字技术深入融合,借助技术创新对现有生产资源进行重组优化[4]。企业数字化转型是对实体经济的传统经营模式的颠覆性改造,对经济发展产生了广泛的影响。现有研究成果从不同角度评估了企业数字化转型的直接影响和溢出效应。企业实现数字

化转型有助于革新经营模式,实现降本增效[5],优化组织架构,增强企业柔性及敏捷性[6]。同时,数字化转型也有助于培育企业创新动能,是企业战略创新的关键路径[7]。企业数字化转型的内外部影响因素众多,大致可分为3类:产业环境因素、制度环境因素、社会环境因素[8]。甄红线等[8]指出,强化知识产权行政保护能显著提升企业的研发投入和数字专利申请量,推动数字化转型进程。然而,企业数字化转型也面临众多挑战。刘淑春等[5]发现,受限于转型能力欠缺、成本高昂及适应期漫长等因素,许多企业倾向于维持现有模式和管理制度,陷入转型意愿不足、能力缺失和风险规避的困境。余典范等[9]认为,数字化转型具有显著的技术外溢效应和正外部性,这反而可能降低企业主动转型的积极性。

(二)网络安全风险管理研究现状

当前,网络安全风险管理领域尚处于发展初期,理论与实务均未成熟,相关概念的定义也未达成共识,近年学界出现了多种术语描述相关概念,如网络安全风险管理、信息安全风险管理和网络安全管理等[10]。为统一表述并防止歧义,本文借鉴Eling等[10]的做法,统一采用"网络安全风险管理(cybersecurity risk management)"这一术语。该术语用以指代网络安全风险管理所包含的完整流程,具体涵盖风险的识别、分析、处置与监控等核心环节。依据风险管理流程的步骤划分,当前针对网络安全风险管理的研究可主要归类为以下3个方向:网络安全风险识别、网络安全风险分析以及网络安全风险处理。

在网络安全风险识别方面,计算机/数据安全一直都是影响企业运营的重要因素,但是直到1986年莫里斯蠕虫事件的出现才使学术界开始关注网络安全问题。网络安全风险分类和识别主要依据其是否影响信息或信息系统的机密性、可用性、完整性[11]。具体包括:信息外泄主要破坏机密性、服务阻断和勒索软件攻击威胁到信息的可用性、网页篡改会削弱完整性、网络钓鱼则可能同时危及机密性与完整性。

在网络安全风险分析方面,相关文献主要集中在具有某些特征的公司更可能遭遇网络安全风险事件,以及一旦发生可能对企业造成的负面影响。例如,Lenging等[12]关注了2004—2012年发生的各种网络安全漏洞事件,发现较小公司容易被入侵,而拥有更好治理体系的公司则不容易受到网络攻击;企业社会责任履行情况较好的企业同样能够降低发生网络安全泄露的风险。Kamiya等[13]的研究则表明,企业的多种特征,如存续年限、市场价值、盈利水平、资本性支出、并购活动、无形资产规模等,均可能成为网络安全风险的潜在诱因。Bose等[14]发现投资者和股东会对企业发生的网络安全事件作出负面反应。

在网络安全风险处理方面,现有研究大多聚焦于网络安全风险的缓解和转移两个方面。在风险缓解方面,现有文献重点探讨了相关技术、模型构建及其产生的溢出效应[10]。在风险转移方面,网络安全保险近年来关注度上升,但既有研究多集中于概念框架、模拟研究和发展现状等方面[15]。由于网络安全风险呈现出多变性、复杂性、关联性和巨灾性特征,网络安全保险的承保双方在被保企业实际网络安全风险状况方面面临信息不对称困境。这种状况不仅阻碍了网络安全保险的发展,也在一定程度上掣肘了相关研究的深入。

就实施网络安全风险管理的影响而言,Gatzer等[2]通过文本分析法实证研究了银行和保险业实施网络安全风险管理对企业价值的影响,发现实施网络安全风险管理能够提高在银行和保险业的价值。田玲等[1]采用文本分析法构建了网络安全意识得分和网络安全风险管理指标,探讨了企业实施网络安全风险管理影响企业价值的作用机制。总体上,相关的学术研究较少。综上所述,已有文献在企业数字化转型的影响因素、网络安全风险管理等方面为本文的研究奠定了良好的基础,但是现有研究在有关数字化转型中的网络安全风险方面的研究仍局限在现象描述,尚缺乏系统的理论和实证研究。本文在已有研究的基础上,将网络安全风险管理与企业数字化转型纳入统一分析框架中,使用文本分析法对上市公司年

报文本信息进行深度挖掘,实证考察实施网络安全风险管理对于企业数字化转型的影响,并探究其潜在影响渠道,从企业所有制、所在行业、所在地区、网络安全意识强弱等方面进行异质性分析,进行了经济后果检验。

(三)研究假设

网络安全风险管理分为风险识别、风险分析和风险处理3 个环节。根据动态能力理论,企业需通过“感知—捕捉—重构”循环应对环境变化[16]。在感知和捕捉到网络安全风险之后,企业能够通过采取适当的网络安全政策和措施以确保有适当和足够的响应能力,可能会直接触发对数字技术的需求[3]。在数字化进程中软件和信息技术构成关键的底层支撑,相关产业的进步能够有效促进企业实现网络化、智能化[9]。同时,此类技术研发的成果往往以数字专利形式体现,数字专利是促进企业数字化转型的核心要素[8]。此外,网络安全风险识别环节需要判断是否影响“信息或信息系统的机密性、可用性或完整性”[11],如果识别到侵权行为,就能进一步采取措施保护企业的数字专利。

目前中国上市公司未被强制要求披露网络安全风险信息,因而外部人士通常难以准确评估企业面临的网络攻击和风险状况。根据信号传递理论,信息披露有助于降低企业内部人员与利益相关者之间的信息不对称,从而提升资本市场的资源配置效率。而管理者自愿披露网络安全风险管理的相关信息,这本身就是传递了一种积极信号,能够降低外部投资者对数字化转型不确定性的担忧,可能吸引长期投资者注入耐心资本,提供长期资金支持,缓解融资约束。长期投资者因其注重长期价值而非短期收益的特点[17],使企业能够承担周期长、高风险的数字化项目,防止管理层因短期业绩压力削减数字化投入,从而保障了企业数字化转型的稳定性。对于投资者而言,未实施网络安全风险管理的企业不披露信息的行为本身也是一种信号,由于投资者难以评估企业对网络安全风险的态度与举措,增加了外部投资者获取信息的成本,最终影响其投资行为[1],从而间接影响企业数字化转型中的长期资金可得性。

此外,网络安全风险管理要求企业将财务与人力资源投入网络安全基础设施,这类投资具有技术专用性与高迭代特征,直接扩大了研发支出规模。具体而言,网络安全技术的开发和应用往往需要企业投入大量资金和人力,以构建防火墙、加密系统、入侵检测系统等专用技术设施。这些技术不仅具有高度的专业性,还需要不断更新迭代以应对日益复杂的网络威胁,推动企业在研发活动中的持续投入。此外,网络安全风险管理的实施可能有助于改变管理层的技术认知与战略导向,提升对技术前沿的感知能力,因此将更多资源分配至长期的创新研发项目,研发资源也可能向人工智能等前沿技术倾斜,推动了研发支出的结构性增长。根据资源基础观,核心资源有助于企业构建竞争优势。甄红线等[8]研究发现,增加研发支出有利于推动企业数字化转型。企业能通过直接拉动研发投入和间接优化资源配置的双重路径,增加研发支出,从而加速数字化转型。

据此,本文提出以下假设。

假设 1:企业实施网络安全风险管理可以促进数字化转型。

二、研究设计

(一)数据说明

本文的初始样本包括 2007—2023 年中国 A 股上市企业。在 2007 年以前,中国企业实施网络安全风险管理的情况较少。2007 年中国网民数量首次突破 2 亿人,互联网普及率突破 15%,网络应用场景的扩展与安全风险的暴露同步激增。同年国家颁布的《信息安全等级保护管理办法》等政策首次确立了分级防护框架,引起社会各界广泛关注,助推了企业实施网络安全风险管理的进程。因此,本文以 2007 年为样本的起始年。网络安全风险相关和数字化转型的指标通过对上市公司年报的文本分析获取,控制变量数据来源于 CSMAR 数据库。按照以下步骤对样本进行处理:①剔除交易状态为 ST 的企业;②剔除相关数据缺失的观测样本;③为了降低极端值对实证结果的影响,除

二元变量以外，其余变量均作了1%双向缩尾处理。最后得到符合本文要求的36 736个企业—年度样本。

（二）变量测度

1. 数字化转型

本文借鉴吴非等[18]的做法，建立了包含“人工智能技术”“区块链技术”“云计算技术”“大数据技术”“数字技术应用”5类关键词的企业数字化转型词库。基于Python对上市企业年报文本提取关键词，分类归集词频并形成最终加总词频，鉴于总词频数据右偏分布的特征，进行对数化处理后得到企业数字化转型程度这一指标。

2. 网络安全风险管理

本文借鉴田玲等[1]的做法，筛选出可以反映企业实施了网络安全风险管理的关键词，如表1所示。通过文本分析法，在上市企业年报中搜索关键词，判断企业是否实施网络安全风险管理，并构建网络安全风险管理变量。该变量为0～1变量，若企业实施了网络安全风险管理则赋值为1，反之则赋值为0。

表1　网络安全风险管理关键词

分类	关键词
网络安全风险管理	网络安全、网络安全风险、网络安全管理、网络风险管理、网络安全风险管理、信息安全、信息安全管理、信息安全风险管理、计算机安全、计算机安全管理、首席信息安全官、CISO、首席信息官、CIO、IT风险、IT安全、IT风险管理、IT安全管理、网络安全保险、信息安全保险

3. 控制变量

参考已有文献[2]，本文选取以下企业层面控制变量：企业年龄（*Age*）、企业规模（*Size*）、杠杆率（*Leverage*）、资产回报率（*ROA*）、增长率（*Growth*）、资本不透明度（*Opacity*）、企业所有制（*SOE*）、两职合一（*Duality*）、总经理持股比例（*CEOShare*）、股权集中度（*Top*1）。各个变量的含义及计算公式见表2。

（三）模型设定

本文重点考察实施网络安全风险管理对企业数字化转型的影响，并构建如下模型展开分析：

$$Digital_{ijt} = \alpha_1 Cyber\_RM_{ijt} + \beta_n \times Z^n_{ijt} + \gamma_j + \delta_t + \varepsilon_{ijt} \quad (1)$$

表2　变量定义及详细说明

变量代码	变量名称	含义及计算方式
Digital	数字化转型程度	年报中关键词出现的频数，取自然对数
Cyber_RM	网络安全风险管理	实施网络安全风险管理，赋值1；否则，赋值0
Age	企业年龄	样本所在年份与成立年份之差，取对数
Size	企业规模	期末总资产的自然对数
Leverage	杠杆率	期末总负债除以总资产
ROA	资产收益率	净利润占总资产比例
Growth	增长率	本年营业收入除以上年营业收入再减1
Opacity	资本不透明度	无形资产占总资产账面价值比例
SOE	企业所有制	国有资本控股定义为国有企业，赋值1；否则，赋值0
Duality	两职合一	CEO是否兼任董事长，兼任赋值1；否则，赋值0
CEOShare	管理层持股比例	董监高持股数量占总股数量之比
*Top*1	股权集中度	第一大股东持股比例

其中，i代表企业，j代表行业，t代表年份，解释变量为实施网络安全风险管理的二元变量（$Cyber\_RM_{ijt}$），被解释变量为企业数字化转型程度（$Digital_{ijt}$）。Z^n_{ijt}为企业层面的控制变量组，γ_j为行业固定效应，δ_t为年份固定效应，ε_{ijt}为误差项，假设其服从正态分布。本文重点关注α_1这一参数，如果α_1在统计上显著为正，则说明企业推行网络安全风险管理，能够有效推动其数字化转型进程。鉴于企业在不同年份间的观测值可能存在关联性，本文将标准误聚类在企业层面。

三、实证结果及分析

（一）描述性统计

根据2007—2023年年报的文本分析结果，实施网络安全风险管理的企业数量总体呈现上升趋势。如表3所示，截至2023年，在观测样本中已实施网络安全风险管理的企业—年度观测值共计5 912个，而尚未实施相关管理的企业—年度观测值

表3　实施网络安全风险管理的企业数量变化情况

年份	*Cyber_RM*=0	*Cyber_RM*=1	样本量	年份	*Cyber_RM*=0	*Cyber_RM*=1	样本量
2007	985	54	1 039	2016	1 819	237	2 056
2008	989	79	1 068	2017	1 955	286	2 241
2009	1 112	96	1 208	2018	2 041	352	2 393
2010	1 139	82	1 221	2019	2 410	484	2 894
2011	1 307	115	1 422	2020	2 370	533	2 903
2012	1 639	131	1 770	2021	2 400	723	3 123
2013	1 807	175	1 982	2022	2 515	976	3 491
2014	1 805	195	2000	2 023	2 797	1 189	3 986
2015	1 734	205	1939	—	—	—	—

共计 30 824 个。主要变量的描述性统计结果见表 4。样本企业的网络安全风险管理(*Cyber_RM*)平均值为 0.160 9,表明样本企业中有 16.09% 的上市企业实施了网络安全风险管理。

表 4　主要变量的描述性统计

变量	样本量	均值	标准差	最小值	中位数	最大值
Digital	36 736	1.159 7	1.414 6	0.000 0	0.693 1	5.010 6
Cyber_RM	36 736	0.160 9	0.367 5	0.000 0	0.000 0	1.000 0
Age	36 736	2.871 1	0.349 4	1.791 8	2.890 4	3.526 4
Size	36 736	22.223 5	1.288 4	19.591 5	22.059 2	26.141 6
Leverage	36 736	0.448 6	0.208 0	0.063 8	0.441 5	0.971 2
ROA	36 736	0.030 6	0.069 7	-0.308 4	0.033 0	0.204 6
Growth	36 736	0.158 3	0.432 4	-0.614 9	0.093 5	2.779 9
Opacity	36 736	0.047 0	0.052 4	0.000 0	0.033 2	0.327 9
SOE	36 736	0.392 4	0.488 3	0.000 0	0.000 0	1.000 0
Duality	36 736	0.264 1	0.440 8	0.000 0	0.000 0	1.000 0
CEOShare	36 736	11.006 1	17.694 1	0.000 0	0.183 0	65.769 4
*Top*1	36 736	0.337 6	0.146 0	0.090 0	0.313 1	0.738 0

(二)基本回归结果

表 5 汇报了实施网络安全风险管理对企业数字化转型影响的基准回归结果,其中回归(1)仅包括实施网络安全风险管理这一核心解释变量,回归(2)加入了影响企业数字化转型的其他控制变量,回归(3)~(4)依次加入了年份固定效应和行业固定效应。核心解释变量的系数在 1% 的统计水平上始终显著为正,表明实施网络安全风险管理对企业数字化转型产生了积极影响。随着更多维度的控制变量纳入模型,回归结果仍然显著,证实了前文结果的稳健性。从企业的层面来看,实施网络安全风险管理确实可以促进数字化转型,由此验证了本文的假设 1。从控制变量来看,企业规模(*Size*)、总经理持股比例(*CEOShare*)、两职合一(*Duality*)与企业数字化转型程度均显著正相关,而杠杆率(*Leverage*)、资产回报率(*ROA*)、股权集中度(*Top*1)、企业所有制(*SOE*)与企业数字化转型程度均显著负相关。说明企业规模越大、总经理持股比例越高、CEO 与董事长两职兼任的企业往往数字化转型程度较高,杠杆率、资产回报率、股权集中度越高和国有制企业往往数字化转型程度较低。

表 5　企业网络安全风险管理对数字化转型的影响

变量	(1)	(2)	(3	(4)
	Digital	*Digital*	*Digital*	*Digital*
Cyber_RM	1.580 3***	1.395 0***	1.299 7***	0.634 8***
	(0.043 5)	(0.042 8)	(0.043 0)	(0.033 2)
Age	—	0.392 2***	-0.233 8***	-0.072 7
		(0.041 2)	(0.053 9)	(0.045 4)
Size	—	0.173 1***	0.078 3***	0.155 1***
		(0.012 6)	(0.012 9)	(0.010 8)
Leverage	—	-0.759 9***	-0.327 4***	-0.147 4**
		(0.080 5)	(0.080 4)	(0.064 4)
ROA	—	-1.632 6***	-0.845 7***	-0.398 6***
		(0.175 7)	(0.172 4)	(0.136 3)
Growth	—	0.032 7**	0.036 5**	0.019 6
		(0.016 7)	(0.016 4)	(0.014 3)
Opacity	—	-1.183 8***	-1.134 1***	0.052 9
		(0.246 1)	(0.242 5)	(0.223 1)
SOE	—	-0.354 7***	-0.183 4***	-0.138 4***
		(0.035 5)	(0.034 9)	(0.028 9)
Duality	—	0.185 4***	0.131 2***	0.077 1***
		(0.032 3)	(0.031 4)	(0.024 7)
CEOShare	—	0.007 4***	0.003 2***	0.001 4*
		(0.001 0)	(0.001 0)	(0.000 8)
*Top*1	—	-0.518 3***	-0.504 1***	-0.173 7**
		(0.107 0)	(0.103 6)	(0.078 8)
_cons	0.9054***	-3.412 5***	0.274 1	-2.031 1***
	(0.0162)	(0.259 3)	(0.318 6)	(0.272 0)
年份	否	否	是	是
行业	否	否	否	是
N	36 736	36 736	36 736	36 719
调整 R^2 值	0.168 5	0.244 0	0.297 4	0.522 6

注:***、**、* 分别表示在 $p < 0.01$、$p < 0.05$、$p < 0.10$ 时有统计学意义。下同。

(三)内生性分析

1. Bartik 工具变量法

本文借鉴余振等[19]的做法,构建一个 Bartik 工具变量。其基本思路是,用分析单元的份额构成和总体的增长率来模拟出历年的估计值,该估计值与实际值高度相关,但是与其他的残差项不相关。在本文中,以滞后一期($Cyber\_RM_{i,j,t-1}$)作为初始份额,用 $G_{j,t}$ 表示企业所在行业的网络安全风险管理水平增长率,代表外生冲击,构建 *BartikIV* 如式(2)所示。本文认为行业层面的网络安全风险管理水平不会明显地受到个体企业数字化转型的影响,是相对外生的;单个企业层面,除了网络安全风险管理以外的冲击也可能导致估计偏误,但是只要单个企业没有重要到其内部冲击影响到整个行业层面的网络安全风险管理水平,*BartikIV* 就是有效的。

$$BartikIV = Cyber\_RM_{i,j,t-1} \times (1 + G_{j,t}) \quad (2)$$

表 6 第(1)列汇报了使用工具变量的两阶段回归结果。其中第一阶段回归结果的 F 统计量均大于 10% 偏误水平下 Stock-Yogo 的临界值,表明不存在弱工具变量问题。KP - LM 统计量也大于 1% 显著性水平的临界值,拒绝了工具变量识别不足的原假设。第二阶段结果显示,使用工具变量

后,网络安全风险管理的系数依然显著为正,表明在考虑了内生性问题之后,网络安全风险管理依然对企业数字化转型产生显著正向影响,与基准回归结果一致,说明上述回归结论基本稳健和基本可靠。

2. 倾向得分匹配法

本文采用倾向得分匹配法进一步检验实施 *Cyber_RM* 对企业数字化转型程度的影响。具体做法如下:首先,以实施网络安全风险管理的企业为实验组,以未实施网络安全风险管理的企业为控制组;其次,通过企业年龄(*Age*)、企业规模(*Size*)、杠杆率(*Leverage*)、资产回报率(*ROA*)、增长率(*Growth*)、资本不透明度(*Opacity*)、企业所有制(*SOE*)、两职合一(*Duality*)、总经理持股比例(*CEOShare*)、股权集中度指标(*Top*1)等变量,借助 Logit 模型为实施 *Cyber_RM* 的样本匹配未实施 *Cyber_RM* 的样本;再次,对样本进行 1∶1、无放回、半径为 0.01 的近邻匹配;最后,对匹配留下的样本进行回归,回归结果见表 6。其中,第(2)列汇报了 PSM 匹配后的回归结果,*Cyber_RM* 系数为 0.643 6,在 1% 的水平上显著为正。这一结果表明,在控制了样本选择偏差和控制变量的差异后,研究结论仍然成立。

表 6　工具变量检验结果

变量	(1) 工具变量回归		(2) 倾向得分匹配法
	第一阶段 *Cyber_RM*	第二阶段 *Digital*	*Digital*
IV_Bartik	0.486 6*** (0.009 3)	—	—
Cyber_RM	—	1.053 5*** (0.063 6)	0.643 6*** (0.038 2)
控制变量	是	是	是
年份	是	是	是
行业	是	是	是
KP-F 统计量	2 717.58 {16.38}	—	—
KP-LM 统计量	676.29 [0.000]	—	—
N	21 711	21 711	10 202
调整 R^2 值	0.469 6	0.072 0	0.571 7

3. 处理效应模型

自选择偏差本质是因遗漏变量而导致的内生性问题。本文借鉴 Maddala[20] 提出的处理效应模型来缓解不可观测因素导致的自选择偏差问题。在第一阶段回归中,借鉴田玲等[1]的做法,构造网络安全意识(*CyberRiskAware*)这一变量作为外生工具变量。然后使用 Probit 回归得到各个样本的拟合值 $\hat{y_i}$,并计算得到逆米尔斯比率(IMR)。在第二阶段回归中,将逆米尔斯比率作为控制变量,引入原回归方程中,回归结果见表 7。表 7 第(1)列汇报了直接使用两步估计法的结果,*lambda* 显著为负,说明存在自选择偏差问题。第一阶段 *CyberRiskAware* 的系数显著为正,表明选择方程中的工具变量有效。第二阶段中 *Cyber_RM* 系数显著为正,验证了实施网络安全风险管理对企业数字化转型的正向影响效果。第(2)列汇报了手工完成两步估计法的结果,并且在第二阶段回归中加入了年份固定效应和行业固定效应,聚类到企业层面。第一阶段回归结果与(1)相同,第二阶段在使用更严格的固定效应后 *Cyber_RM* 系数显著为正。第(3)列汇报了使用极大似然估计(MLE)从模型整体角度对参数进行估计,并聚类到企业层面,以减少效率损失[21]。*lambda* 的估计系数为 -0.515 5,*rho* 的 wald 检验结果说明至少在 1% 的水平下拒绝原假设,同样说明确实存在自选择偏差。第一阶段 *CyberRiskAware* 的系数显著为正,验证了选择方程

表 7　处理效应回归结果

变量	(1)	(2)		(3)
	直接使用两步估计法	手工完成两步估计法第一阶段	手工完成两步估计法第二阶段	MLE
Digital 回归结果				
Cyber_RM	3.414 1*** (0.085 9)	—	1.619 8*** (0.118 8)	2.277 2*** (0.143 5)
IMR	—	—	-0.561 5*** (0.063 8)	—
_cons	-2.159 3*** (0.155 7)	—	-1.392 2*** (0.275 9)	-2.864 9*** (0.273 0)
控制变量	是	—	是	是
Cyber_RM 回归结果				
CyberRiskAware	0.859 8*** (0.025 2)	0.859 8*** (0.025 2)	—	0.967 7*** (0.045 3)
_cons	-4.467 3*** (0.166 6)	-4.467 3*** (0.166 6)	—	-4.057 4*** (0.332 2)
控制变量	是	是	是	是
lambda	-1.172 7*** (0.047 9)	—	—	-0.515 5 (0.037 2)
athrho	—	—	—	-0.430 6*** (0.067 1)
lnsigma	—	—	—	0.239 2*** (0.013 9)
年份	否	否	是	否
行业	否	否	是	否
N	36 736	36 736	36 719	36 736

中的工具变量的有效性。此时第二阶段 *Cyber_RM* 系数仍然显著为正。以上结果表明,实施网络安全风险管理对企业数字化转型的正向影响效果是稳健的。

(四)稳健性检验

1. 替换因变量

通过重新量化数字化转型来进行稳健性检验。首先,借鉴赵宸宇等[22]使用文本分析和专家打分相结合的方法,使用熵值法进行权重调整,使测算结果更贴合实际,重新生成企业数字化转型变量(*Digital_A*);其次,借鉴张永珅等[23]的研究方法,利用公司财务报告附注披露的年末无形资产明细项中与数字化技术相关部分占无形资产总额的比例,重新生成企业数字化转型变量(*Digital_B*)。基于 *Digital_A* 、*Digital_B* 的回归结果分别在表 8 第(1)列、第(2)列中给出,其中 *Cyber_RM* 的系数在 1% 水平上显著为正,验证了结果的稳健性。

2. 替换自变量

考虑到直接采用 *Cyber_RM* 这一 0 - 1 变量作为解释变量,可能存在一定偏误。因此,本文进一步统计网络安全风险管理关键词在企业年报中出现的总频数,并对频数进行归一化处理,构建网络安全风险管理有效性(*Cyber_RM_A*)这一指标,加入稳健性检验,回归结果如表 8 第(3)列所示,其中 *Cyber_RM_A* 的系数在 1% 水平上显著为正,进一步验证了结果的稳健性,也表明网络安全风险管理越有效,越能助推企业数字化转型。

3. 采取更严格的固定效应

为排除潜在因素的干扰,本文虽已加入年份及行业固定效应,但地区层面的特定因素未必能被完全捕捉,如地区网络攻击事件等,可能会影响研究结果的可靠性和普适性。因此,本文进一步引入企业所在省份的固定效应,以确保更全面地控制可能影响研究结果的地区相关因素。表 8 的第(4)列回归结果显示,*Cyber_RM* 的系数在 1% 水平上显著为正,从而验证了研究结果的稳健性。

4. 剔除 2007—2012 年样本和平衡面板

本文主要通过对上市公司年报进行文本分析来构建数字化转型指标,但以“人工智能技术”“区块链技术”等方面的关键词测算样本初期的数字化转型程度可能不准确,所以剔除 2007—2012 年样本,仅保留 2013—2023 年样本数据进行回归,有助于增强模型对核心变量关系的识别精度,验证主回归结果是否在更稳定的子样本中保持一致性。表 8 的第(5)列回归结果显示,*Cyber_RM* 的系数在 1% 水平上显著为正,从而验证了研究结果的稳健性。在剔除 2007—2012 年样本的基础上,只保留 2013—2023 年各项数据均无缺失的样本企业,转换为平衡面板进行回归。平衡面板能够通过统一时间跨度与个体观测,确保个体可比性,使参数估计更稳定。尽管可能损失部分样本,但其核心价值在于通过标准化数据结构验证核心假设的可靠性。平衡面板回归结果如表 8 的第(6)列所示,*Cyber_RM* 的系数仍然在 1% 水平上显著为正。以上稳健性检验结果都表明,企业实施网络安全风险管理对数字化转型的正向影响效果是稳健的。

表 8　稳健性检验结果

变量	替换因变量度量方式		替换自变量度量方式	增加省份固定效应	剔除部分样本	剔除后平衡面板
	(1) *Digital_A*	(2) *Digital_B*	(3) *Digital*	(4) *Digital*	(5) *Digital*	(6) *Digital*
Cyber_RM	0.013 6*** (0.000 8)	0.036 6*** (0.005 2)	—	0.580 0*** (0.052 2)	0.677 0*** (0.035 3)	0.708 3*** (0.064 1)
Cyber_RM_A	—	—	3.069 0*** (0.941 3)	—	—	—
_cons	-0.032 4*** (0.005 8)	0.494 7*** (0.055 5)	-2.311 1*** (0.286 1)	-2.259 7*** (0.388 2)	-2.335 8*** (0.313 9)	-1.918 9*** (0.617 4)
控制变量	是	是	是	是	是	是
年份	是	是	是	是	是	是
行业	是	是	是	是	是	是
省份	否	否	否	是	否	否
N	36 719	35 468	36 719	19 934	29 007	10 780
调整 R^2 值	0.452 4	0.286 3	0.502 9	0.489 1	0.480 6	0.483 9

(五)异质性分析

1. 基于企业所有制的异质性

考虑到国有企业和非国有企业在网络安全风险管理方面的差异,本文探究了不同企业所有制的情况下,实施网络安全风险管理对企业数字化转型的影响是否存在差异。根据实际控制人属性将样本企业分为国有企业(*SOE* =1)和非国有企业(*SOE* =0)两种类型,将企业是否国有企业与实施网络安全风险管理的交乘项(*CRM_SOE*)加入模型进行检验,回归结果如表 9 的第(1)列所示,交乘项系数在 1% 的水平上显著为负。说明相较于国有企业,非国有企业开展网络安全风险管理对企业数字化转型产生了显著的促进作用。这或可解释为:国有企业因规模与系统复杂性等因素面临路径依赖,内在变革动力不足,可能抑制其数字化转型。而非国有企业经营以利润为导向,在实施网络安全风险管理的过程中,对科技前沿的敏感度更高,从而能够增强资金的靶向性、提升企业的数字化创新实力,从而更好地推动数字化转型。

2. 基于行业技术变化速度的异质性

考虑到行业的差异可能对网络安全风险管理发挥的作用有较大影响,本文借鉴田玲等[1]的做法,将电气机械及器材制造业(行业代码:C38),计算机、通信和其他电子设备制造业(行业代码 C39),通用仪器仪表制造业(C40)标记为技术更新变化速度快(*Tech*)的行业[24],赋值为 *Tech* =1,其他行业的企业样本赋值 *Tech* =0。将企业是否处于技术更新变化速度快的行业与实施网络安全风险管理的交乘项(*CRM_Tech*)加入模型进行检验,回归结果如表 9 的第(2)列所示,交乘项系数在 1% 的水平上显著为正。说明在技术更新变化速度快的行业,实施网络安全风险管理对企业数字化转型的促进作用更强。对此可能的解释是在高频技术更迭行业中,新兴技术的快速应用使企业面临更复杂的安全漏洞和未知风险,倒逼企业建立前瞻性网络安全防护体系。而市场竞争压力会强化网络安全投入的正外部性,加速数字化生态系统的资源整合和成果落地,因此对数字化转型的推动效果更显著。

3. 基于区域的异质性

为了更好地对比处于不同地区的企业的结果,本文借鉴汪晓文等[25]的做法将 30 个省份划分为东部和中西部两个地区。东部地区包括北京市、上海市、天津市、辽宁省、河北省、山东省、江苏省、浙江省、福建省、广东省、广西壮族自治区和海南省 12 个省份,中西部地区为剩余 18 个省份。如果企业所在省份处于东部地区,赋值 *Is_east* =1,如果企业所在省份处于中西部地区,赋值 *Is_east* =0。将企业所在省份是否处于东部地区与实施网络安全风险管理的交乘项(*CRM_east*)加入模型进行检验,回归结果如表 9 的第(3)列所示,交乘项系数在 1% 的水平上显著为正。说明相较于中西部地区,东部地区企业实施网络安全风险管理对数字化转型的促进作用更强。对此可能的解释是东部地区的数字基础设施和资源禀赋较好,并且由于市场化进程较早,具有良好的竞争环境,有利于激发企业数字化创新能力,有利于减少企业数字化转型过程中受到的约束。而中西部地区因资源禀赋相对落后、市场竞争相对不激烈等一系列制约因素,使得网络安全风险管理对企业数字化转型的促进作用尚未得到充分的发挥。

4. 基于网络安全意识强弱的异质性

考虑到企业网络安全意识的强弱可能对网络安全风险管理发挥的作用有影响,本文将网络安全意识(*CyberRiskAware*)高于样本企业年度均值的观测标记为网络安全意识较强(*HighRiskAware* =1),低于样本企业年度均值的观测标记为网络安全意识较弱(*HighRiskAware* =0)。将企业网络安全意识强弱与实施网络安全风险管理的交乘项(*CRM_aware*)加入模型进行检验,回归结果如表 9 第(4)列所示,交乘项系数在 10% 的水平上显著为正。说明,网络安全意识较强的企业开展网络安全风险管理对企业数字化转型的推动效果更显著。对此可能的解释是,网络安全意识是企业实施网络安全风险管理的重要前提条件[2],网络安全意识与网络安全风险管理之间的关系本质上涉及意识与行为之间的关系,意识决定行为,网络安全意识较强的企业往往建立了更成熟的风险评估机制,网络安全风险管理的水平更高,能够在数字化转型过程中前瞻性地识别技术应用中的安全隐患,通过动态优化实施方案降低转型阻力,让实施网络安全风险管理对数字化转型的促进作用得到充分的发挥。

表 9　异质性分析

变量	(1)	(2)	(3)	(4)
	Digital	*Digital*	*Digital*	*Digital*
Cyber_RM	0.694 1*** (0.039 3)	0.517 9*** (0.036 8)	0.400 7*** (0.077 3)	0.594 6*** (0.033 8)
CRM_SOE	−0.167 5*** (0.061 0)	—	—	—
SOE	−0.114 8*** (0.028 6)	—	—	—
CRM_tech	—	0.418 8*** (0.074 4)	—	—
Tech	—	0.168 7 (0.130 3)	—	—
CRM_east	—	—	0.266 5*** (0.101 0)	—
Is_east	—	—	0.010 3 (0.031 0)	—
CRM_aware	—	—	—	0.133 3* (0.071 3)
HighRiskAware	—	—	—	0.233 5*** (0.051 0)
_cons	−2.067 3*** (0.271 6)	−2.050 0*** (0.271 4)	−2.337 9*** (0.380 4)	−2.009 4*** (0.271 0)
控制变量	是	是	是	是
年份	是	是	是	是
行业	是	是	是	是
N	36 719	36 719	19 934	36 719
调整 R^2 值	0.523 0	0.524 6	0.481 0	0.524 9

(六)渠道检验

1. 推动数字专利申请

借鉴甄红线等[8]的做法,将上市公司专利的主分类号与国家统计局发布的《数字经济及其核心产业统计分类(2021)》进行匹配,得到上市公司各年度内的数字专利申请数量,加 1 取自然对数后得到指标企业数字经济发明专利申请量(*Digital_patent*),作为衡量企业数字专利申请的指标。表 10 第(1)列回归结果显示,*Cyber_RM* 与 *Digital_patent* 显著正相关,表明实施网络安全风险管理有助于推动企业数字专利申请,提升企业的数字技术创新能力。进一步地,第(2)列结果表明,*Digital_patent* 与 *Digital* 的回归系数显著为正,表明企业数字专利申请有助于数字化转型,与已有研究结论一致。上述结果支持了前文的推测,表明促进企业数字专利申请是实施网络安全风险管理影响企业数字化转型的一个潜在影响渠道。

2. 提高长期机构投资者持有比例

借鉴刘京军等[26]的做法,根据机构交易的换手率特征划分长期投资者和短期投资者,换手率越大的机构投资者定义为短期投资者,换手率越小的定义为长期投资者,对样本企业的机构投资者类型计算长期机构投资者的持有比例(*LIO*)。表 10 第(3)列回归结果显示,*Cyber_RM* 与 *LIO* 显著正相关,表明实施网络安全风险管理有助于提高长期机构投资者持有比例。但第(4)列的 *LIO* 回归系数为负,无法说明提高长期机构投资者持有比例能够对企业数字化转型产生正向作用。因此,无法验证提高长期机构投资者持有比例是实施网络安全风险管理影响企业数字化转型的渠道。

3. 增加研发投入

同样借鉴甄红线等[8]的做法,采用企业研发支出占主营业务收入的比例(*RD*)衡量企业研发投入。表 10 第(5)列回归结果显示,*Cyber_RM* 与 *RD* 显著正相关,表明实施网络安全风险管理有助于增加企业研发投入。而第(6)列结果显示,*RD* 与 *Digital* 的回归系数显著为正,表明企业数字专利申请有助于数字化转型,与已有结论一致。上述结果支持了前文的推测,表明增加研发投入是实施网络安全风险管理影响企业数字化转型的一个潜在影响渠道。

表 10　渠道检验结果

变量	(1)	(2)	(3)	(4)	(5)	(6)
	Digital_patent	*Digital*	*LIO*	*Digital*	*RD*	*Digital*
Cyber_RM	0.393 9*** (0.034 0)	—	0.001 8*** (0.000 6)	—	0.014 9*** (0.001 5)	—
Digital_patent	—	0.179 4*** (0.011 7)	—	—	—	—
LIO	—	—	—	−0.621 4** (0.293 3)	—	—
RD	—	—	—	—	—	2.150 9*** (0.376 0)
_cons	−9.505 8*** (0.402 6)	−0.604 0** (0.297 6)	−0.135 6*** (0.007 2)	−2.432 4*** (0.298 3)	0.102 3*** (0.012 6)	−2.629 7*** (0.355 6)
控制变量	是	是	是	是	是	是
年份	是	是	是	是	是	是
行业	是	是	是	是	是	是
N	36 719	36 719	35 562	35 562	26 953	26 953
调整 R^2 值	0.506 6	0.518 2	0.191 7	0.501 3	0.430 2	0.474 6

(七)经济后果检验

前文的研究结果表明,企业实施网络安全风险管理,促进了数字专利的申请和研发支出的增加,从而正面影响企业数字化转型。以往研究表明,开展数字化转型,可助力企业激发创新活力并优化全要素生产率[22]。作为考察企业长期经济增长的重要指标,企业全要素生产率的来源及核算方式包括劳动效率的改善、技术进步率以及规模经济效应,因此本文进一步考虑实施网络安全风险管理对数字化转型的促进作用能否进一步提升企业全要素生产率,其中全要素生产率(*TFP_OP*)采用 OP 法进行测算。此外,采用同年度资产回报率(*ROA*)及营业收入增长率(*Growth*)来衡量企业短期绩效,考察实施网络安全风险管理对数字化转型的促进作用对企业短期绩效的影响。本文参考张勇等[27]的做法,将实施网络安全风险管理与数字化转型的交乘项(*Digital_CRM*)加入检验,分别从资产回报率、营业收入增长率、全要素生产率三方面进行经济后果检验。

回归结果如表 11 所示。第(2)列和第(4)列显示,当被解释变量为 *ROA* 和 *Growth* 时,交乘项 *Digital_CRM* 的系数均显著为负,这说明企业实施网络安全风险管理对数字化转型的促进作用对企业短期内的资产回报率、营业收入增长率产生负面影响,这可能是因为网络安全风险管理和数字化转型可能伴随高昂的固定成本,短期内可能超过其带来的收益,反而恶化企业财务绩效。当被解释变量为 *TFP_OP* 时,交乘项 *Digital_CRM* 的系数显著为正,说明企业实施网络安全风险管理对数字化转型的促进作用能够进一步提升企业的全要素生产率,提高资源利用效率,增强企业的长期竞争力和可持续发展能力,对企业长期发展产生积极影响。

表 11　经济后果检验

变量	(1)	(2)	(3)	(4)	(5)	(6)
	ROA	*ROA*	*Growth*	*Growth*	*TFP_OP*	*TFP_OP*
Cyber_RM	-0.001 3 (0.001 5)	0.004 6** (0.002 1)	-0.005 1 (0.006 3)	0.006 8 (0.010 1)	0.023 3 (0.015 3)	-0.028 9 (0.023 1)
Digital_CRM	—	-0.002 7*** (0.000 9)	—	-0.006 8* (0.003 9)	—	0.017 0* (0.010 3)
Digital	—	-0.000 4 (0.000 6)	—	0.003 9 (0.002 7)	—	0.024 4*** (0.006 7)
_cons	-0.163 0*** (0.014 3)	-0.165 0*** (0.014 4)	-0.071 3 (0.058 7)	-0.067 7 (0.059 2)	-3.724 2*** (0.176 4)	-3.670 8*** (0.176 4)
控制变量	是	是	是	是	是	是
年份	是	是	是	是	是	是
行业	是	是	是	是	是	是
N	36 719	36 719	36 719	36 719	35 816	35 816
调整 R^2 值	0.141 7	0.142 2	0.091 6	0.091 6	0.649 3	0.650 2

四、结论与政策启示

本文以中国上市企业为样本,利用文本分析法构建网络安全风险管理和数字化转型指标,就实施网络安全风险管理对企业数字化转型的影响效应和作用机理展开了实证分析。基准回归结果表明,在控制了年份和行业固定效应后,实施网络安全风险管理对企业数字化转型产生了显著的促进作用,内生性检验和稳健性检验结果均表明,网络安全风险管理对企业数字化转型影响始终显著为正。异质性检验结果发现,网络安全风险管理对数字化转型的正向影响在非国有制的、处于技术更新变化速度快的行业的、所在省份处于东部地区、网络安全意识强的企业分组相对较强。进一步的作用机制表明,网络安全风险管理能力的提高,促进了企业数字专利的申请和企业研发支出的增加,上述因素均为实施网络安全风险管理对于企业数字化转型的潜在影响渠道。经济后果检验发现,实施网络安全风险管理对于企业数字化转型的促进作用可能恶化企业短期绩效,但能够进一步提升企业的全要素生产率,对企业长期发展产生积极影响[28]。

根据研究结果,本文提出以下政策建议。①各地政府应顺网络安全风险管理深化之势而为,在强化数字基础设施安全底座的同时,借助网络安全风险管理能力全流程、全要素赋能企业数字化转型,以技术标准建设为重点、产业链协同为抓手,分层分类支持非国有与技术密集型企业,针对中小微企业与战略性新兴行业实施差异化扶持政策。推动东部技术资源向中西部梯度渗透,缩小区域数字能力鸿沟。②企业应该增强网络安全风险意识,强化对于网络安全风险的识别、分析、处理意识,积极实施网络安全风险管理,将网络安全

风险管理纳入战略决策中枢,建立风险量化评估模型与动态预警系统,提升企业应对网络安全风险事件的不确定性的能力,不断更新迭代以应对日益复杂的网络威胁,确保在数字化时代保持竞争力。提高企业资源配置效率,确保网络安全风险管理策略与企业长期发展目标一致,从而实现可持续发展和风险最小化。③企业应该根据自身行业发展背景、所在地区、财务状况,有针对性地构建适合自身需求的网络安全风险管理模式,应该加强技术认知和战略导向,提升对科技前沿的敏感度,增加研发支出,引进高质量人力资本,强化与科研机构的技术联合攻关,建立网络安全专利池与技术转化绿色通道,加速技术成果向产业应用落地,为企业数字化转型破解瓶颈,提高全要素生产率,使得实施网络安全风险管理对于数字化转型的促进效应得到更大的发挥。

参考文献:

[1]田玲,崔靖茹,王正文. 网络安全意识、网络安全风险管理和企业价值 [J]. 保险研究, 2024 (4): 3-19.

[2]GATZER T N, SCHUBERT M. Cyber risk management in the US banking and insurance industry: a textual and empirical analysis of determinants and value [J]. The journal of risk and insurance, 2022, 89(3): 725-763.

[3]CAVUSOGLU H, MISHRA B, RAGHUNATHAN S. The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers [J]. Journal of electronic commerce, 2004, 9(1): 70-104.

[4]袁淳,肖土盛,耿春晓,等. 数字化转型与企业分工:专业化还是纵向一体化 [J]. 中国工业经济, 2021(9): 137-155.

[5]刘淑春,闫津臣,张思雪,等. 企业管理数字化变革能提升投入产出效率吗 [J]. 管理世界, 2021, 37(5): 170-190,13.

[6]池毛毛,王伟军,卢新元,等. 数字商务战略剖面和组织重构能力关系的研究:究竟是抑制还是促进? [J]. 管理工程学报, 2020, 34(4): 11-20.

[7]王福胜,郑茜月,张东超. 数字化转型、国际化战略与企业创新 [J]. 运筹与管理, 2024, 33(9): 120-125.

[8]甄红线,王玺,方红星. 知识产权行政保护与企业数字化转型 [J]. 经济研究, 2023, 58(11): 62-79.

[9]余典范,王超,陈磊. 政府补助、产业链协同与企业数字化 [J]. 经济管理, 2022, 44(5): 63-82.

[10] ELING M, MCSHANE M, NGUYEN T. Cyber risk management: history and future research directions [J]. Risk management and insurance review, 2021, 24(6): 93-125.

[11]BIENER C, ELING M, WIRFS J. Insurability of cyber risk: an empirical analysis [J]. The Geneva papers on risk and insurance- issues and practice, 2015, 40(1): 131-158.

[12] LENGING C, MINNICK K, SCHOMO P. Corporate governance, social responsibility, and data breaches [J]. Financial review, 2018, 53(2): 413-455.

[13]KAMIYA S, KANG J, KIM J, et al. Risk management, firm reputation, and the impact of successful cyberattacks on target firms [J]. Journal of financial economics, 2021, 139(3): 719-749.

[14] BOSE I, LEUNG A. Do phishing alerts impact global corporations? a firm value analysis [J]. Decision support systems, 2014, 64(8): 67-78.

[15]董坤祥,谢宗晓,甄杰,等. 基于数据泄露类型的网络信息安全风险度量与可保性研究 [J]. 保险研究, 2019(11): 25-41.

[16]TEECE D J. Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance [J]. Strategic management journal, 2007, 28(13): 1319-1350.

[17]LATHAM S F, BRAUN M R. Managerial risk, innovation, and organizational decline [J]. Journal of management, 2009, 35(2): 258-281.

[18]吴非,常曦,任晓怡. 政府驱动型创新:财政科技支出与企业数字化转型 [J]. 财政研究, 2021(1): 102-115.

[19]余振,李萌,庄额嘉. Bartik 工具变量法在因果识别中的应用与检验 [J]. 数量经济技术经济研究, 2025, 42(1): 200-220.

[20] MADDALA G S. Limited-dependent and qualitative variables in econometrics [M]. London: cambridge university press, 1986: 212-217.

[21]王正文,李委铮,但钰宛,等. 全面风险管理与企业融资约束[J]. 经济评论, 2023(5): 144-164.

[22]赵宸宇,王文春,李雪松. 数字化转型如何影响企业全要素生产率[J]. 财贸经济, 2021, 42(7): 114-129.

[23]张永珅,李小波,邢铭强. 企业数字化转型与审计定价 [J]. 审计研究, 2021(3): 62-71.

[24]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.

[25]汪晓文,陈明月,陈南旭. 数字经济、绿色技术创新与产业结构升级[J]. 经济问题,2023 (1):19-28.

[26]刘京军,徐浩萍. 机构投资者:长期投资者还是短期机会主义者? [J]. 金融研究, 2012(9): 141-154.

[27]张勇,贾静雯. 企业绿色信贷的绿色创新效应研究:来自文本分析方法度量的绿色信贷证据 [J]. 金融论坛, 2024, 29(8): 59-69,80.

[28] MCSHANE M, NGUYEN T. Time varying effects of cyberattacks on firm value [J]. The geneva papers on risk and insurance-issues and practice, 2020, 45 (4): 580-615.

(本文责编:润　泽)