数字化转型中信息安全协同治理对企业竞争优势的影响

甄　杰[1]，谢宗晓[2]，董坤祥[3]，林润辉[4]
1 重庆工商大学 管理科学与工程学院，重庆 400067
2 中国金融认证中心 法律与合规部，北京 100054
3 山东财经大学 管理科学与工程学院，济南 250014
4 南开大学 商学院，天津 300071

摘要：数字化转型是企业更好感知并满足外部市场需求，实现和精进内部数字化运营管理的必由之路。然而，企业数字化转型中频繁发生的数据泄露等信息安全事件不仅给企业造成严重经济损失，而且危及社会稳定和国家安全，暴露了企业数字化转型中信息安全治理滞后于现实需要的突出矛盾，已有研究对此没有给予足够关注。

基于资源基础理论，从信息安全的价值创造功能出发，探讨企业数字化转型中信息安全协同治理对企业竞争优势的影响，并重点分析信息安全整合能力与信息安全应急能力在此过程中的中介作用，以验证信息安全治理－信息安全能力－价值创造的理论逻辑。面向国内 136 家推进数字化转型的企业收集调查问卷，采用结构方程模型 (SEM) 和模糊集定性比较分析 (fsQCA) 的混合研究方法对提出的研究假设进行实证检验。

研究结果表明，①信息安全协同治理、信息安全整合能力、信息安全应急能力均对企业竞争优势有显著正向影响，三者形成了企业竞争优势的两类前因构型；②信息安全整合能力、信息安全应急能力在信息安全协同治理与企业竞争优势关系中起部分中介作用；③对比来看，信息安全整合能力对企业竞争优势的影响效应大于信息安全应急能力的影响效应，且两者的互补效应不显著。

研究结果明确了信息安全治理－信息安全能力－价值创造理论逻辑的合理性，证实了企业数字化转型中信息安全协同治理对企业竞争优势的积极影响，拓展了对信息安全整合能力、信息安全应急能力的理论认知。同时，从推进信息安全协同治理、提升信息安全整合能力和信息安全应急能力等方面提出的对策建议，对企业合理且有效管控数字化转型中的信息安全风险具有现实的指导意义。

关键词：数字化转型；信息安全协同治理；信息安全整合能力；信息安全应急能力；竞争优势

中图分类号：C93　　**文献标识码**：A　　**doi**：10.3969/j.issn.1672－0334.2024.04.004

文章编号：1672－0334(2024)04－0039－14

收稿日期：2022－07－12　　**修返日期**：2024－01－31

基金项目：国家自然科学基金 (72102025)；国家社会科学基金 (21CGL017)；重庆市社会科学规划项目 (2021NDYB083)；重庆市教委科学技术研究项目 (KJQN202100842)

作者简介：甄杰，管理学博士，重庆工商大学管理科学与工程学院副教授，研究方向为信息安全治理、企业数字化转型等，代表性学术成果为“信息安全治理与企业绩效：一个被调节的中介作用模型”，发表在 2020 年第 1 期《南开管理评论》，E-mail：zhenjie@vip.126.com

谢宗晓，管理学博士，中国金融认证中心法律与合规部副研究员，研究方向为网络与信息安全管理等，E-mail：xiezongxiao@vip.163.com

董坤祥，管理学博士，山东财经大学管理科学与工程学院副教授，研究方向为网络安全保险等，代表性学术成果为“强制性约束下企业信息安全投资与网络保险的最优决策分析”，发表在 2021 年第 6 期《中国管理科学》，E-mail：dkxgood@163.com

林润辉，管理学博士，南开大学商学院教授，研究方向为信息安全治理等，E-mail：linrh@nankai.edu.cn

引言

在数字技术推动的新一轮科技革命背景下，企业迫切需要通过数字化转型提高生产和经营效率[1]，以增强自身的市场竞争力[2]。企业数字化转型是指通过将数字技术引入已有企业管理架构[3]，推动信息结构、管理方式、运营机制、生产和决策过程的重塑，实现企业数字化运营管理的过程[4]。尽管数字化转型能够为企业创造巨大商业价值，但也会形成一些新的信息安全风险场景和风险诱因[5]，进而引发数据泄露等信息安全事件，不仅给企业造成严重经济损失[6]，甚至危及社会稳定和国家安全。因此，如何科学防范和化解企业数字化转型中的信息安全风险成为近几年业界和学界共同关注的热点问题。

信息安全治理是企业管控数字化转型中信息安全风险的有效途径，但在具体实践中面临两个亟待解决的矛盾：第一，企业内部存在追求数字化转型绩效与追求信息安全之间的冲突，导致部分管理者质疑信息安全的价值。第二，企业各部门对信息安全的重视程度和管理策略不一致，造成企业整体信息安全水平不高[7]。这两个矛盾与企业信息安全关键治理要素的缺失有关系，即由谁在什么状态下实施何种信息安全措施的问题不明确。因此，本研究从系统治理视角出发，探讨数字化转型中信息安全协同治理对企业竞争优势的影响，阐明信息安全协同治理的逻辑和价值，揭示信息安全协同治理提升企业竞争优势的机理。本研究有助于完善企业信息安全治理理论，同时为企业数字化转型中的信息安全治理实践提供科学依据。

1 相关研究评述

企业数字化转型中的信息安全风险管理问题已经受到不少国内外学者的关注，已有研究主要集中在三个方面：第一，探讨信息安全投资抑制数据泄露等信息安全事件的有效性[8]。这类研究认为加大对硬件设施等技术手段的投资能够有效减少由企业外部网络攻击导致的数据泄露风险，减少企业信息安全风险损失[9]。第二，研究企业高层管理团队成员的IT技能对数据泄露等信息安全事件的影响。这类研究得出企业高管团队成员 (如CEO、CIO) 的IT技能越高，越有利于企业对数据泄露等信息安全事件的防范和处置[10]，而且有助于提高企业数字化转型中的信息安全水平[11]。第三，分析企业如何构建并完善面向数字化转型的信息、网络与数据安全管理体系[12]。这类研究表明，企业信息安全管理的程序化、标准化、相关认证和对内部员工开展信息安全培训等措施，不仅能有效减少信息安全风险发生的可能性[13]，而且能降低风险发生后的经济损失[14]。

尽管已有研究为面向数字化转型的企业信息安全管理研究提供了有益借鉴，但还存在以下三方面局限：第一，缺乏从系统整体视角分析企业数字化转型中信息安全风险管理的研究。企业各类生产要素的数字化和各项管理工作的智能化，使得企业数字化转型中的信息安全风险几乎涉及所有部门或所有业务流程的所有环节，让信息安全成为一项复杂的系统工程[15]。这就需要从系统整体视角出发，采用基于多元主体的协同治理思维防范和化解各类信息安全风险。第二，较少涉及企业信息安全能力的探讨。企业数字化转型中的信息安全风险具有广泛的业务相关性，一旦发生信息安全事件将导致企业数字化运营管理停滞[16]，亟需构建和提升信息安全能力以合理应对和处置各类潜在信息安全风险。第三，忽视了信息安全的价值创造功能。在企业数字化运营管理中，数据等关键信息资源是企业的战略性资产，面向数字化转型的信息安全已经成为企业价值创造的新途径。显然，能够确保信息资产安全的企业可以更快、更好地适应数字经济发展，在市场竞争中取得优势[17]。

基于上述分析，本研究基于系统治理思维，探讨企业数字化转型中信息安全协同治理是否能够有效提升信息安全能力，进而帮助企业创造竞争优势的理论命题。换言之，本研究尝试验证信息安全治理－信息安全能力－价值创造的内在逻辑和作用机理。本研究的创新之处主要体现在两方面：第一，针对已有研究对企业数字化转型中信息安全能力探讨的不充分[18]，分析信息安全协同治理如何影响常规状态下的信息安全整合能力、非常规状态下的信息安全应急能力，为企业数字化转型中的信息安全能力建设[19]提供新的理论观点。第二，针对已有研究中较少涉及信息安全的价值创造功能，本研究采用结构方程模型 (SEM) 和模糊集定性比较分析 (fsQCA) 的混合研究方法识别并深入分析企业竞争优势的影响组态，明确信息安全协同治理提升企业竞争优势的路径和机理，为数字化运营管理下的企业信息安全治理研究提供新的结论及理论依据。

2 理论分析和研究假设

2.1 理论研究框架

本研究基于资源基础理论 (resource-based theory, RBV) 构建研究框架，资源基础理论认为企业是各类资源的集合，这些资源囊括能够展现企业竞争力的任何事物，既可以是有形的资产，也可以是无形的资产，企业之间由于资源异质性往往存在明显的绩效差异[20]。实际上，资源基础理论包括两个基本观点：第一，不同企业所拥有的优势资源存在差异[20]，如技能和能力、专利技术、研发投入、人力资源、关系网络和制度资源等[21]。第二，优势资源往往在企业之间具有不可复制性，即便能够复制也要需要一定的时间周期，因此基于不同资源所形成的绩效差异可以持续一段时间[22]。所以，企业基于自身资源和能力所形成的竞争优势也需要根据外部市场环境的动态变化进行适应性调整，不能一劳永逸[23]。

资源基础理论认为组织的竞争优势与其所拥有的资源和能力密不可分，其中资源是用于生产的投入要素，能力是运用资源完成任务的各项技能的集

合[24]。据此，本研究尝试做出信息安全治理－信息安全能力－价值创造的理论推演。首先，信息安全协同治理作为组织内部防范和化解信息安全风险的一种制度安排或制度资源，有助于企业构建信息安全能力。由于企业数字化运营管理中的信息安全风险几乎涉及数字技术应用的所有场景，而信息安全协同治理作为一种能够协调不同部门或业务流程之间信息安全活动的制度逻辑及其安排，有助于企业明确各部门和各流程的信息安全职责和权限，从而实现信息安全相关资源的合理布局，构建良好的信息安全能力。其次，信息安全能力作为一种关键的信息资源保护能力有利于企业创造竞争优势。在企业数字化运营管理背景下，以数据为代表的信息资源愈发重要，良好的信息安全能力既可以确保常规状态下企业各部门或流程偏差性信息安全活动的出现，又能够在面对突发信息安全风险时做出合理应对。常规状态下的信息安全整合能力和突发状态下的信息安全应急能力作为信息安全能力的两种形式，均有助于确保企业关键信息资产的安全，使企业可以基于自身良好的信息安全能力获取持续的市场竞争优势。

2.2 信息安全协同治理与企业竞争优势

信息安全治理是指在满足合规要求基础上，将信息安全融入各项业务中，以实现信息安全与转型战略的一致性匹配，确保信息安全风险得到有效管控的制度安排[25]。信息安全协同治理是企业信息安全治理在数字化转型中的一种具体应用模式，它强调不同部门或业务流程需要就信息安全形成一致性认识并采取共同行动，这是因为数字化运营管理下的信息安全几乎涉及所有部门的所有环节，如果存在明显的短板会导致企业整体信息安全的表现大打折扣。信息安全治理包括以下关键环节：①员工注重识别信息安全风险征兆并报告部门领导。②部门领导对所报告风险进行研判，如有必要则报告给高管团队。③高管团队或信息安全领导小组就此展开协同探讨[26]。④倘若面对企业内部难以解决的信息安全风险，则向第三方机构求助，以改进企业信息安全保障措施和处置程序。需要说明的是，由于篇幅所限，本研究暂不探讨涉及第三方机构解决信息安全风险的情况。企业信息安全协同治理模式的基本逻辑见图 1。

面对信息安全风险发生的不确定性和影响范围的广泛性等特点[27]，跨部门建立起来的信息安全协同治理能够将多元相关主体纳入其中，协调不同主体在处理信息安全风险过程中的关系。首先，信息安全风险征兆出现后，为了有效抑制风险在企业内部横向或纵向的传播，员工需要主动向部门领导报告这一风险异常情况。其次，员工和部门领导在经过分析之后，如果满足风险报送条件，则需要将感知后的风险报于高管团队。最后，高管团队针对信息安全风险进行深度讨论并达成处理意见，然后给出明确的应对举措。在此过程中，IT 部门和信息安全

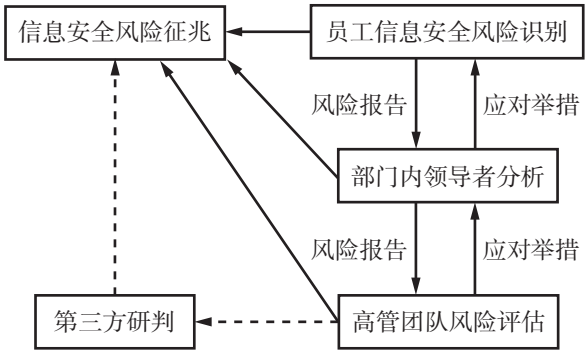


图 1 企业信息安全协同治理模式的基本逻辑

Figure 1 The Basic Logic of Information Security Collaborative Governance Model

部门在对信息安全风险处置意见上发挥关键作用。因此，信息安全协同治理可以协调不同部门的相关主体在处置信息安全风险时的行为，促进企业信息安全管理的科学化、规范化和标准化，这将显著提高企业的信息安全水平，进而提升企业竞争优势[28]。因此，本研究提出假设。

H_1 信息安全协同治理对企业竞争优势具有显著正向影响。

2.3 信息安全整合能力的中介作用

信息安全整合能力是指企业为了满足信息安全管理要求，通过识别、配置、协调和优化信息资源以及信息安全行动，实现不同部门或流程之间对接和信息共享的能力[15]。在数字化转型中，信息安全整合能力不仅可以帮助企业快速整合内部信息安全资源，而且能够有效防控各类潜在信息安全的威胁以及数据安全风险，形成与信息资源重要程度相匹配的常规状态下的信息安全能力。参考已有研究，本研究从识别信息安全要求、配置信息安全资源、协调信息安全活动和优化信息安全风险控制措施 4 个方面深入分析企业信息安全整合能力[15]。

识别信息安全要求是为了确保企业信息安全管理满足监管和合规需要。配置信息安全资源的目的是保证信息安全管理所需的人力、财力、物力能够及时到位。协调信息安全活动是为了使不同部门或流程的信息安全活动同步。优化信息安全风险措施是为了将风险控制在企业能够接受的范畴和水平内[15]。因此，信息安全整合能力可以增强企业对外部复杂信息安全环境的适应能力，并据此调整和优化企业内部的信息安全资源配置[29]，良好的信息安全管理状态有助于企业提高竞争优势及其绩效表现[30]。

企业信息安全协同治理明确了相关各方的信息安全风险责任和应对措施，明晰了相关各方的信息安全风险报送程序和研判机制，这有利于实现企业不同部门与业务流程之间信息安全活动的对接和信息共享。也就是说，信息安全协同治理强调相关各方的合作、对接与协同，通过整合各方的信息安全资源和信息安全活动来共同应对信息安全威胁，这一过程无形之中生成和发展了企业的信息安全整合能

力。此外，来自高管团队的信息安全风险研判能够在高层管理层面释放信息安全重要性的信号，这同样有助于协调企业信息安全资源，协同优化相关各方的信息安全活动，提升信息安全整合能力。

一方面，信息安全整合能力通过整合和优化相关各方的信息资源，可以更加可靠、高效地管理和保护企业重要信息资产，降低信息安全风险事件发生的可能性，提高企业整体的信息安全水平，这种可靠的信息安全能力可以为企业提供竞争优势。另一方面，企业信息安全整合能力强调相关各方共同应对信息安全风险，这有助于企业各部门或业务流程不同环节之间建立更加密切的合作关系，实现企业对客户和市场安全需求的敏捷响应，使企业在行业中更具竞争力。因此，本研究提出假设。

H_2 信息安全整合能力在信息安全协同治理与企业竞争优势关系之间起中介作用。

2.4 信息安全应急能力的中介作用

企业信息安全应急能力是在非常规状态下管控网络、数据等突发信息安全风险事件发生及其造成的损害，保障企业关键信息资产安全的一种能力[31]，它是对企业信息安全整合能力在非常规状态下的一种有力补充。一般而言，重大信息安全突发事件往往会造成企业信息系统大面积瘫痪，导致企业数字化运营管理的中断。因此，企业对信息安全突发事件的处理程序应确保及时有效，这需要具备健全、完善的信息安全突发事件处理程序和应对步骤[32]。因此，企业信息安全应急能力既要包括应急预警，又要包括衍生风险的评估和应对等基本规则[33]。

首先，企业信息安全协同治理模式所搭建的高管团队风险评估、部门领导和员工协同分析的管理体系，能够为网络和信息安全应急处置工作的规划、推进和落实提供规范管理制度、安全策略和相关流程，这有助于提高企业信息安全应急能力。其次，企业信息安全协同治理所明确的相关各方职责和权限，建立起的信息安全事件的报告和处理机制能够确保及时有效地处理信息安全事件。最后，企业信息安全协同治理所倡导的各部门信息共享、互动合作和信息安全活动一致性，能够确保相关各方获取最新的安全威胁情报和风险管控应对措施，从而提高企业信息安全应急能力。

在企业数字化运营管理变得愈发重要的背景下，如果企业展现出良好的信息安全应急能力，能够快速应对并解决信息安全事件，将赢得客户和合作伙伴的信任和认可，提升企业的声誉和竞争力。另外，信息安全应急能力可以提升企业的业务连续性。当企业遭受信息安全事件时，如果能够迅速恢复业务运营，减少停工和停产时间，将有助于保持企业的正常运转。与此同时，市场相关各方可以感受到企业经营的稳定性和可靠性，增强对企业的信任和合作，这将为企业带来持续的市场机会和竞争优势。可见，健全的信息安全应急能力有助于减少信息安全突发事件造成的损失和危害，确保企业关键信息资源安全，维护企业数字化运营管理的正常运转，最终能够提高企业竞争优势。因此，本研究提出假设。

H_3 信息安全应急能力在信息安全协同治理与企业竞争优势关系之间起中介作用。

2.5 交互效应

企业数字化转型面临着日益复杂的网络和信息安全形势，信息安全整合能力能够在常规状态下实现不同部门或流程之间的信息安全对接和信息共享，更加侧重在防；而信息安全应急能力可以在非常规突发状态下控制信息安全风险造成的损失，更加侧重在控。两者在促进企业数字化转型中竞争优势方面可能存在互补效应，主要理由如下：第一，信息安全风险具有广泛性、不确定性等特点，在企业信息安全协同治理中需要构建整合能力和应急能力，两者是平衡的，这种互补机制将促进企业竞争优势的产生。第二，在与企业竞争优势的关系中，两者互为对方与企业竞争优势关系间的调节变量，信息安全整合能力对信息安全应急能力与企业竞争优势之间的关系具有调节作用，信息安全整合能力越强，信息安全应急能力与企业竞争优势之间的关系越强，信息安全应急能力越强，信息安全整合能力与企业竞争优势之间的关系越强。因此，本研究提出假设。

H_4 信息安全整合能力和信息安全应急能力在提升企业竞争优势中具有互补作用，即信息安全整合能力正向调节信息安全应急能力与企业竞争优势之间的关系；信息安全应急能力正向调节信息安全整合能力与企业竞争优势之间的关系。

综上所述，本研究提出的研究模型如图 2 所示。

3 研究设计

3.1 研究方法

本研究采用 SEM 和 fsQCA 相结合的混合研究方法验证研究假设，原因包括以下两个方面：第一，由于 SEM 仅能根据固定变量路径进行简单统计验证[34]，因此，本研究进一步采用 fsQCA 对前因变量影响企业竞争优势的不同组态进行分析。第二，由于本研究对企业数字化转型的研究情境设定，一些没有明确内部数字化转型策略的样本企业被排除在外，导致样本企业数量相对较小，而 Smart PLS 3.0 在数据分析和模型验证上更适合小样本分析[35]。另外，fsQCA 3.0 在数据分析上整合了定性和定量的优势，对样本数量的要求比较宽松[36]。因此，基于 SEM 和 fsQCA 的混合研究方法可以保证研究模型和实证数据的匹配性，提高研究结果的可信性，而且三角测量能够使本研究的研究结果更加稳健。

3.2 样本来源

本研究通过问卷调查收集数据，数据的收集过程分为两个阶段：第一阶段于 2019 年 8 月至 12 月，在相关行业协会和第三方认证机构帮助下发放问卷 320 份。为了保证样本企业正在开展数字化转型相关工作，在问卷中依据数据成熟度相关要点增加数字化转型筛选问题。同时，参与者主要为 IT 部门负

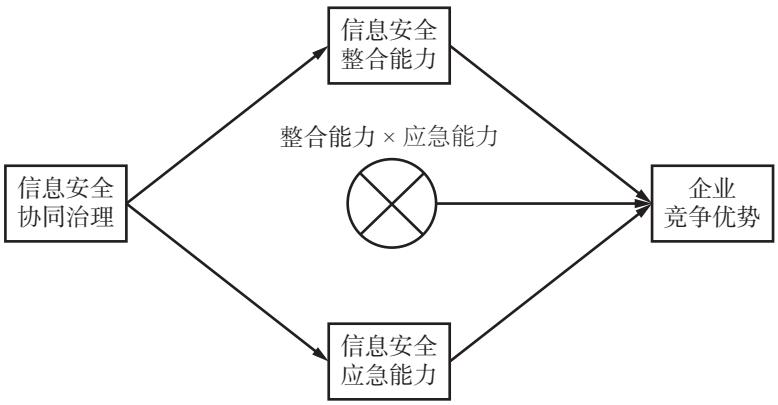


图 2 研究模型

Figure 2 Research Model

责人和经理，或者为分管 IT 部门工作的总经理，以确保参与者了解企业的数字化转型的实际情况。本阶段的调查工作侧重在样本企业内部数字化转型推进中的基本问题，调查内容涵盖自变量相关内容，共回回收有效问卷 173 份。第二阶段的数据收集工作于 2020 年 6 月至 8 月，向第一阶段的 173 家企业进行二次问卷调查，每家企业发放一份问卷，本阶段调查工作侧重于了解样本企业数字化转型的影响效应，调查内容主要涉及因变量相关内容。之所以间隔一段时间开展二次调查，是因为信息安全协同治理影响效用的发挥需要一定周期[37]，本阶段调查共回收有效问卷 136 份。

描述性统计结果显示，在行业类型方面，金融相关企业 71 家，占比为 52.206%；软件相关企业 39 家，占比为 28.676%；包含智能制造的制造相关企业 15 家，占比为 11.029%；通信相关企业 6 家，占比为 4.412%；电子商务相关企业 5 家，占比为 3.677%。在企业规模方面，从业人员大于等于 500 人的企业 33 家，占比为 24.265%；从业人员在 100 人至 500 人的企业 88 家，占比为 64.706%；从业人员小于等于 100 人的企业 15 家，占比为 11.029%。

3.3 变量测量

为了保证变量测量的准确性和有效性，本研究均采用已有研究中被广泛使用和验证的量表，并在咨询金融和制造行业从业人员基础上，根据企业数字化转型的研究情境进行必要修正。同时，本研究采用以下两个措施保证问卷简洁，确保问卷被不同行业参与者理解：第一，邀请一位企业管理研究领域的教授和两位拥有多年从业经验的企业高管阅读问卷中的问题并提出修改意见。第二，将修改后的问卷小范围发放给 20 名左右的硕士研究生，以检验问卷的结构效度。调查问卷采用 Likert 5 点评分法，1 为非常不同意，5 为非常同意，所有变量所包含的具体测量题项见表 1。

(1) 因变量：企业竞争优势。参考吴松强等[38]和肖勰等[39]的测量量表并进行修改，用于测量企业竞争优势。由于研究情境的差异，上述两项研究在对企业竞争优势测量方面各有侧重，研究团队在咨询了行业从业人员和信息系统领域学者的基础上最终确定从降低成本、增加收入和提升效率 3 个主要维度测量企业通过企业数字化转型获取的相对于竞争对手的有利条件和战略优势。

(2) 自变量：信息安全协同治理。参考 PRASAD et al.[40]的量表并进行修改，用于测量信息安全协同治理，结合企业数字化转型的要求确定 4 个题项，分别测量企业数字化转型中员工与部门领导之间、部门领导与高管团队之间、高管团队多个成员之间和企业跨部门或跨流程的信息安全沟通和协同 4 方面内容。

(3) 中介变量：信息安全整合能力和信息安全应急能力。对信息安全整合能力的测量采用甄杰等[15]的测量量表，包括 4 个题项，分别测量企业数字化转型中识别内外部的信息安全要求、配置与关键信息资产相匹配信息安全资源、协调内部不同部门之间的信息安全活动和优化企业的信息安全风险控制措施 4 个方面的情况。对信息安全应急能力的测量，首先依据《国家网络安全事件应急预案》的指导意见确定整体方向和基本原则，其次结合应急能力评估[41]和应急能力形成[42]的相关研究成果，最终确定从预警监测、应急处置、事后恢复和总结反馈 4 方面调查企业信息安全应急能力的内容。

(4) 控制变量：行业类型和企业规模。企业隶属行业不同，对数字化转型的需求和深入程度不同，不同行业之间企业推进数字化转型的进程也存在差异，这可能对企业竞争优势产生影响。企业规模与其在行业内的影响力具有一定关系，因此企业对数字化转型的重视程度不同，这同样可能对企业竞争优势产生影响。因此，本研究将行业类型和企业规模作为控制变量。

4 数据分析和假设检验

4.1 共同方法偏差检验

基于问卷调查的实证研究中，如果一份问卷中的所有问题均由同一位参与者回答可能导致共同方法

表1 量表的信度和效度

Table 1 Reliability and Validity of Scales

变量	题项	因子载荷	*AVE*	*CR*	Cronbach′s α
企业竞争优势	1 企业能以更低的成本提供产品或服务	0.858	0.727	0.889	0.813
	2 企业具备更好的市场盈利能力	0.837			
	3 企业能够更加快速有效地满足客户需求	0.864			
信息安全协同治理	1 员工与部门领导间有信息安全沟通机制	0.806	0.712	0.908	0.865
	2 部门领导与高管团队间有信息安全共识	0.821			
	3 高管团队各成员共同采取信息安全活动	0.885			
	4 不同部门/流程间就信息安全展开协作	0.863			
信息安全整合能力	1 企业能够识别外部信息安全管理要求	0.781	0.611	0.863	0.789
	2 企业可以合理配置信息安全各项资源	0.783			
	3 企业善于协调不同部门的信息安全活动	0.773			
	4 企业进行信息安全风险防控措施的优化	0.794			
信息安全应急能力	1 企业能够检测并预警信息安全风险	0.835	0.656	0.884	0.826
	2 企业可以对信息安全风险进行应急处置	0.812			
	3 企业存在信息安全风险后的恢复机制	0.844			
	4 企业会对信息安全风险进行事后总结	0.749			

偏差，影响到研究结果的准确性。本研究采用事前控制和事后检验相互结合的方式，对可能存在的共同方法偏差进行排除和检验。在事前控制方面，本研究采取了如下措施：①根据已有研究中被广泛验证的成熟量表生成调查问题，表述清晰且明确。②在收集问卷时，尽管一份问卷是由同一位参与者完成，但因变量和自变量采用不同的时间周期进行收集，能够排除参与者情绪和工作状态等个人主观特征对问卷填写效果产生的消极影响。在事后检验方面，本研究采取了如下措施：①采用Harman单因素测量方法对136份有效问卷进行共同方法偏差分析，得到第一个主成分因子的贡献率小于40%的阈值设定，满足检验要求。②采用标签变量方法，选择相关系数最低的一项，计算每个变量的偏相关系数[34]，检验结果同样满足要求。因此，本研究调查数据不存在明显的共同方法偏差。

4.2 信度和效度检验

本研究采用组合信度 (*CR*) 和Cronbach′s α 检验问卷的信度，通过验证性因子分析检验结构效度，同时采用平均抽取变异量 (*AVE*) 评价量表的聚合效度，各指标结果见表1。此外，本研究采用潜变量*AVE*的平方根是否大于潜变量之间的相关值检验区分效度，检验结果见表2。

由表1可知，企业竞争优势的*CR*值为0.889，信息安全协同治理的*CR*值为0.908，信息安全整合能力的*CR*值为0.863，信息安全应急能力的*CR*值为0.884，均大于0.700的基本要求。4个变量对应的Cronbach′s α 值为0.813、0.865、0.789和0.826，均大于0.700的基本要求。综合两项指标数值，说明问卷具有良好的信度水平。与此同时，4个变量的*AVE*分别为0.727、0.712、0.611和0.656，均大于0.500的基本要求，体现了较高的聚合效度水平。

由表2可知，企业竞争优势、信息安全协同治理、信息安全整合能力和信息安全应急能力4个变量的*AVE*的平方根均大于各变量之间的相关系数，表明问卷具有较好的区分效度。另外，本研究还对4个变量测量题项之间的交叉因子载荷进行检验，检验结果见表3。表3的数据显示，因子载荷在所属潜变量一列的值要明显高于其他潜变量的值，说明测量模型具有较高的聚合效度和区分效度。综上所述，本研究采用的变量测量量表具有较好的信度和效度水平。

对于将行业类型和企业规模作为控制变量纳入到研究模型进行检验，由于本研究中分析的样本量相对较少，因此采用LIANG et al.[43]推荐的分析方法对其进行二次检验，即每次检验只涉及到一个控制变量。检验结果显示，行业类型的系数为0.168，$p < 0.050$，企业规模的系数为0.040，$p > 0.050$，即行业类型对企业竞争优势具有一定影响，而企业规模对企业竞争优势的影响不显著。

表 2 潜变量均值、方差和 *AVE* 的平方根

Table 2 Means, Variance, and *AVE* Square Root of Latent Variable

	均值	标准差	企业竞争优势	信息安全协同治理	信息安全整合能力	信息安全应急能力
企业竞争优势	3.534	0.926	**0.852**			
信息安全协同治理	3.437	1.002	0.546	**0.843**		
信息安全整合能力	3.605	0.851	0.571	0.595	**0.781**	
信息安全应急能力	3.682	0.849	0.513	0.497	0.584	**0.809**

注: 对角线黑体数据为对应变量*AVE*的平方根。

表 3 交叉载荷检验结果

Table 3 Test Results for Cross Loading

测量题项	企业竞争优势	信息安全协同治理	信息安全整合能力	信息安全应急能力
企业竞争优势 1	**0.868**	0.528	0.575	0.596
企业竞争优势 2	**0.843**	0.474	0.578	0.543
企业竞争优势 3	**0.847**	0.436	0.530	0.438
信息安全协同治理 1	0.494	**0.814**	0.505	0.474
信息安全协同治理 2	0.470	**0.826**	0.555	0.453
信息安全协同治理 3	0.504	**0.882**	0.531	0.467
信息安全协同治理 4	0.434	**0.853**	0.526	0.383
信息安全整合能力 1	0.534	0.564	**0.797**	0.522
信息安全整合能力 2	0.387	0.441	**0.754**	0.568
信息安全整合能力 3	0.595	0.493	**0.787**	0.683
信息安全整合能力 4	0.519	0.452	**0.788**	0.530
信息安全应急能力 1	0.440	0.386	0.608	**0.813**
信息安全应急能力 2	0.531	0.466	0.609	**0.820**
信息安全应急能力 3	0.440	0.409	0.577	**0.825**
信息安全应急能力 4	0.577	0.439	0.589	**0.780**

4.3 多重共线性检验

本研究通过检验方差膨胀因子 (*VIF*) 来消除潜在的多重共线性风险, 以确保研究模型的准确性。检验结果显示, 信息安全协同治理、信息安全整合能力和信息安全应急能力的 *VIF* 数值分别为 1.676、2.643 和 2.223, 3 个变量中 *VIF* 数值最高的是 2.643, 远低于 3.300 的阈值要求。因此, 本研究中无需担心变量之间的多重共线性问题。

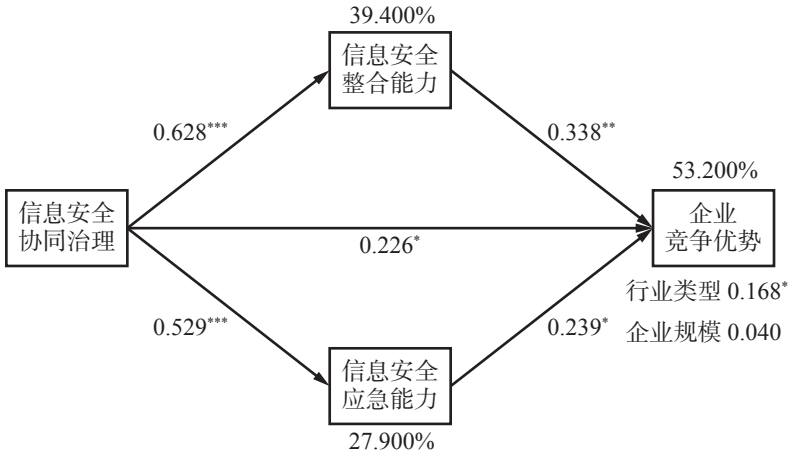
4.4 假设检验

在对中介效应检验之前, 先对变量之间的直接关系进行检验。本研究采用 Smart PLS 3.0 进行结构方程模型检验, 变量之间的直接影响效应结果如图 3 所示。

由图 3 可知, 信息安全协同治理对企业竞争优势具有显著正向影响, $\beta = 0.226$, $p < 0.050$, H_1 得到验证。信息安全协同治理对信息安全整合能力具有显著正向影响, $\beta = 0.628$, $p < 0.001$; 信息安全协同治理对信息安全应急能力具有显著正向影响, $\beta = 0.529$, $p < 0.001$; 信息安全整合能力对企业竞争优势具有显著正向影响, $\beta = 0.338$, $p < 0.010$; 信息安全应急能力对企业竞争优势具有显著正向影响, $\beta = 0.239$, $p < 0.050$。对比来看, 信息安全整合能力对企业竞争优势的影响效用大于信息安全应急能力对企业竞争优势的影响效用。另外, 根据中介变量的作用条件, 再结合上述变量之间的直接关系可以初步推断, 信息安全整合能力、信息安全应急能力可能在信息安全协同治理与企业竞争优势关系中起部分中介作用, 因此, 需要进一步进行验证。

4.5 中介效应检验

本研究采用 bootstrap 方法验证信息安全整合能



注：***为 $p<0.001$，**为 $p<0.010$，*为 $p<0.050$，下同。

图3 PLS全模型分析结果

Figure 3 PLS Full Model Analysis Results

表4 中介效应检验

Table 4 Test Results for Mediating Effects

中介效应影响路径	估计值	标准误差	95%置信区间			
			百分位		偏差校正	
			下限	上限	下限	上限
信息安全协同治理→信息安全整合能力→企业竞争优势	0.208	0.091	0.041	0.405	0.042	0.405
信息安全协同治理→信息安全应急能力→企业竞争优势	0.138	0.063	0.022	0.265	0.031	0.282

力、信息安全应急能力在信息安全协同治理与企业竞争优势关系之间的中介作用。由于该方法具有自抽样方法的明显优势，在中介效应的分析中被广泛运用[44]。在具体操作上，本研究设定bootstrap次数为5 000次，置信区间为95%，由此可得中介效应分析结果，见表4。

由表4可知，在信息安全协同治理→信息安全整合能力→企业竞争优势和信息安全协同治理→信息安全应急能力→企业竞争优势两条中介效应影响路径中，95%置信区间均不包含0，因此，信息安全整合能力、信息安全应急能力在信息安全协同治理与企业竞争优势关系之间的中介作用显著，H_2和H_3得到验证。

4.6 交互效应检验

采用逐步线性回归方法对信息安全整合能力与信息安全应急能力的交互作用对企业竞争优势的影响进行检验，检验结果如表5所示。步骤如下：①模型1以企业竞争优势作为因变量，行业类型和企业规模作为自变量。②模型2在模型1的基础上增加信息安全整合能力作为自变量，结果显示信息安全整合能力对企业竞争优势具有正向影响，$\beta=0.646$，$p<0.001$。③模型3在模型1的基础上增加信息安全应急能力作为自变量，结果显示信息安全应急能力对企业竞争优势具有正向影响，$\beta=0.589$，$p<0.001$。④模型4在模型1的基础上增加信息安全整合能力和信息安全应急能力作为自变量，结果显示信息安全整合能力和信息安全应急能力均对企业竞争优势有正向影响，$\beta=0.463$，$p<0.001$；$\beta=0.248$，$p<0.010$。⑤模型5在模型1的基础上增加信息安全整合能力、信息安全应急能力和两者的交互项作为自变量，结果显示信息安全整合能力与信息安全应急能力的交互项对企业竞争优势的影响不显著，$\beta=-0.226$，$p>0.050$。说明信息安全整合能力和信息安全应急能力在促进企业竞争优势方面不具有互补效应，H_4未得到验证。

H_4未得到验证的结果与本研究的理论预期出现了偏差，即信息安全整合能力与信息安全应急能力的交互效应对企业竞争优势的影响不显著，这可能是由以下两方面原因造成的：第一，企业信息安全整合能力与信息安全应急能力分别属于企业在常态与非常态两种情境下需要具备的信息安全能力，两者之间不具有互补关系，而在一些情况下可能存在替代关系，这需要进行进一步研究。第二，对于推进数字化转型的企业而言，构建适用于数字化运营管理需要的信息安全能力是一个持续的过程，需要逐步予以完善。现阶段，一些企业还没有达到清晰划分出信息安全整合能力和信息安全应急能力的发展水平。

表 5 交互效应检验

Table 5 Test Results for Interaction Effect

变量	企业竞争优势				
	模型1	模型2	模型3	模型4	模型5
信息安全整合能力		0.646***		0.463***	0.604***
信息安全应急能力			0.589***	0.248**	0.391*
信息安全整合能力 × 信息安全应急能力					− 0.270
行业类型	0.177*	0.191*	0.142*	0.172**	0.173**
企业规模	0.063	− 0.012	0.025	− 0.007	0.002
R^2	0.042	0.454	0.385	0.482	0.484
ΔR^2		0.412	− 0.069	0.097	0.002

表 6 变量的校准锚点 (N = 136)

Table 6 Calibration Anchor Points for Variables (N = 136)

变量	企业竞争优势	信息安全协同治理	信息安全整合能力	信息安全应急能力
完全隶属	5	5	5	5
交叉点	3.534	3.347	3.605	3.682
完全不隶属	1	1	1	1

5 模糊集定性比较分析

本研究中的理论模型将企业竞争优势作为因变量，其前因变量包括信息安全协同治理、信息安全整合能力和信息安全应急能力，本研究进一步采用基于组态视角的模糊集定性比较分析方法探讨企业竞争优势的前因构型，以明确前因复杂性和因果非对称关系[45]。

5.1 数据校准

校准是赋予集合隶属度的过程，依据模糊集定性比较分析的步骤，本研究对企业竞争优势、信息安全协同治理、信息安全整合能力和信息安全应急能力 4 个变量进行数据校准，并据此设定完全隶属、交叉点和完全不隶属 3 个临界值。本研究参考已有相关研究的处理方式[46]，在问卷调查中采用 Likert 5 点评分法，5 为完全隶属，1 为完全不隶属，将变量的均值作为交叉点。4 个变量的校准锚点如表 6 所示。

5.2 单个条件必要性分析

本研究采用 fsQCA 3.0 软件对所有前因变量和企业竞争优势的关系进行分析，识别出高企业竞争优势的主要前因构型，并将该结果与 Smart PLS 3.0 的分析结果进行比较。具体而言，本研究首先分析信息安全协同治理、信息安全整合能力和信息安全应急能力对企业竞争优势的必要性条件，按照已有研究的惯例将必要性条件一致性阈值设定为 0.900[47]。检验结果显示，对高企业竞争优势来说，单个条件变量的一致性水平均不高于 0.900，条件变量的必要性分析结果如表 7 所示。因此，信息安全协同治理、信息安全整合能力和信息安全应急能力均不构成单个必要条件。

5.3 组态分析

在高企业竞争优势的前因构型分析中，参考已有相关研究[47]将一致性阈值设置为 0.800，将 PRI 一致性阈值设置为 0.700，将案例频数阈值设定为 1，计算得到高企业竞争优势的结果，见表 8。由表 8 可知，总体一致性为 0.974，覆盖度达到 0.745，均大于设定阈值。同时，研究发现两条获取企业竞争优势的不同路径，包括信息安全协同治理驱动和构建由整合能力与应急能力形成的信息安全能力。

具体来说，产生高企业竞争优势的路径有 3 种组态，即 C_{1a}、C_{1b} 和 C_2。其中，组态 C_{1a} 和组态 C_{1b} 表明通过部署信息安全协同治理、提升信息安全能力和信息安全应急能力均可以获取高企业竞争优势，因此，基于 fsQCA 与基于 SEM 的检验结果基本一致。组态 C_2 表明在信息安全协同治理缺失的条件下，通过构建或提升信息安全整合能力与信息安全应急能力，可以帮助企业获取高企业竞争优势。整体看，上述组态分析结果与假设检验的结果一致。这些结果有利于本研究更好理解企业借助信息安全协同治理构建信息安全整合能力和信息安全应急能力进而培育企业竞争优势的理论逻辑和行动路径。

6 结论

6.1 研究结果

本研究探讨了企业数字化转型中信息安全协同

表7 条件变量的必要性分析

Table 7 Necessary Analysis of Condition Variables

前因条件	一致性	覆盖率
信息安全协同治理	0.798	0.832
信息安全整合能力	0.844	0.835
信息安全应急能力	0.825	0.805

表8 高企业竞争优势的前因构型

Table 8 Antecedent Constructs of Enterprise' High Competitive Advantage

前因条件	产生高企业竞争优势的组态		
	组态C_{1a}	组态C_{1b}	组态C_2
信息安全协同治理	●	●	⊗
信息安全整合能力	●	⊗	●
信息安全应急能力	⊗	●	●
原始覆盖度	0.391	0.337	0.565
唯一覆盖度	0.015	0.024	0.245
一致性	0.940	0.959	0.968
解的覆盖度	0.745		
解的一致性	0.974		

注：●为核心条件存在，⊗为核心条件缺失，●为边缘条件存在，⊗为边缘条件缺失。

治理对企业竞争优势的影响，分析了信息安全整合能力和信息安全应急能力的中介作用以及两者的互补作用，得出以下研究结论。

(1) 企业数字化转型中的信息安全协同治理能够帮助企业创造竞争优势。结果表明，信息安全协同治理对企业竞争优势具有显著正向影响，且证实信息安全协同治理是信息安全整合能力、信息安全应急能力的前因条件。事实上，相关研究已经注意到，良好的网络和信息安全管理水平在提升企业绩效方面的作用[48]，本研究则进一步明确了信息安全能够帮助企业创造价值的内在逻辑。同时，该研究结论拓展了资源基础理论的理论内涵和应用范畴。即在数字经济时代，信息安全将逐渐成为企业的一种重要资源，良好的信息安全不仅能够确保数字化运营管理的进行，而且能够为企业带来良好的行业声誉和竞争优势。

(2) 信息安全整合能力、信息安全应急能力在信息安全协同治理与企业竞争优势关系之间均起部分中介作用。分析发现，信息安全协同治理可以通过信息安全整合能力、信息安全应急能力间接影响企业竞争优势，而且信息安全整合能力对企业竞争优势的影响效用大于信息安全应急能力的影响效用。尽管已有部分研究开始探讨企业信息安全能力对组织绩效的影响[5]，但鲜有研究从常规状态下的信息安全整合能力和突发状态下的信息安全应急能力两方面深入分析信息安全能力的配置。本研究在细化企业信息安全能力的基础上，验证了信息安全整合能力和信息安全应急能力的积极作用。

(3) 企业数字化转型中信息安全整合能力和信息安全应急能力均对企业竞争优势产生积极正向影响，但二者未能形成一种互补关系。在信息安全整合能力和信息安全应急能力的交互检验中，本研究发现信息安全整合能力与信息安全应急能力的交互项对企业竞争优势的影响不显著。这一结论背后的理论逻辑是，信息安全整合能力与信息安全应急能力尽管是企业需要构建的两种能力，但两者之间不具有互补关系，很可能在某些情况下具有相互替代作用，即常规状态下的信息安全能力可能在突发状态下直接转化为信息安全应急能力。该研究结论为企业数字化转型中信息安全整合能力和信息安全应急能力的关系提供了理论参考，也有助于提高企业数字化转型中相关主体关注和提升应急管理和决策能力的理论认识[49]。

6.2 管理启示

上述研究结论对企业有效管控数字化转型中的信息安全风险，通过信息安全协同治理提升信息安全能力和企业竞争优势有以下管理启示。

(1) 企业数字化转型中要重视并推进信息安全协同治理，避免存在短板环节而拖累企业整体信息安全表现。研究结论证实了信息安全协同治理对信息安全整合能力、信息安全应急能力和企业竞争优势的直接影响，并且验证了信息安全协同治理对企业竞争优势的不同影响路径。这体现了信息安全协同治理在企业数字化转型中的作用和效果，因此企业需要重视信息安全协同治理，并推动信息安全协同治理在数字化转型中的落实。举例来说，企业要强化不同部门以及业务流程各环节对关键信息资源的保护，同步各部门的信息安全认知和行动，为企业的数字化运营管理提供安全保障。

(2) 企业需要构建与数字化转型相匹配的信息安全整合能力和信息安全应急能力。研究结果验证了信息安全整合能力、信息安全应急能力在提升企业竞争优势方面的直接效用，以及在信息安全协同治理与企业竞争优势关系之间的间接效用，这充分说明企业构建信息安全能力的必要性。在具体信息管理活动中，企业需要根据所配置的软硬件资源、掌握的运营管理数据、运行的关键信息基础设施等数字化运营的载体，匹配与之相适应的信息安全整合能力和信息安全应急能力，以确保常规和应急状态下技术、系统和数据的安全可靠，避免由于信息资源遭到破坏而导致企业数字化运营管理的中断。

(3) 企业数字化转型中需要注重发挥信息安全协同治理和信息安全整合能力与信息安全应急能力的联动效应，以持续提升企业竞争优势。企业数字化

转型中，需要通过信息安全协同治理部署跨部门、跨流程的信息安全管理措施，提升日常运营管理中的信息安全整合能力，关注自身应对重大信息安全突发事件的应急能力。在推进逻辑上，要注重通过协同治理完善制度和管理策略，并通过严格执行逐渐打造并提升信息安全整合能力和应急能力。此外，在构建信息安全能力过程中需要注意常规状态下的信息安全整合能力与突发状态下的信息安全应急能力的差异，保证信息安全能力建设的合理性和可持续发展。

6.3 研究局限和未来展望

本研究深入探讨了信息安全协同治理对企业竞争优势的影响，尽管研究结论对企业数字化转型中的信息安全风险管控有重要参考价值，但仍然存在以下两方面局限：第一，研究量表的局限性。本研究对于信息安全协同治理、信息安全整合能力、信息安全应急能力和企业竞争优势的 4 个变量的测量均采用已有研究中被使用和验证的量表，没有针对企业数字化转型的特殊性进行量表开发，只是根据数字化转型这一研究情境对原有量表进行部分修正和适应性调整。这难免造成测量量表没有充分反映企业数字化转型的特点，这也是研究团队在未来研究中需要改进的地方。第二，研究样本的局限性。本研究中的样本企业大部分是在行业协会和第三方认证机构的协助下确定的，样本的行业覆盖面显然不够广泛。同时，尽管本研究在问卷中设定筛选问题以尽量保障样本企业正在推进数字化转型的相关工作，但没有办法对不同企业处于数字化转型的哪个阶段进行测量。因此，未来研究需要在行业类型和企业数字化转型发展阶段上开展更为深入的研究。例如，可以针对不同行业内企业数字化转型的信息安全风险治理问题开展案例研究，或者通过扎根理论挖掘企业数字化转型不同阶段信息安全治理的侧重点。

参考文献：

[1] 王一鸣. 百年大变局、高质量发展与构建新发展格局. **管理世界**, 2020, 36(12): 1−12.
WANG Yiming. Changes unseen in a century, high-quality development, and the construction of a new development pattern. ***Journal of Management World***, 2020, 36(12): 1−12.

[2] 马亮, 高峻, 仲伟俊, 等. 数字化转型助力后发企业技术赶超: 企业家精神视角. **管理科学**, 2023, 36(2): 53−74.
MA Liang, GAO Jun, ZHONG Weijun, et al. Digital transformation facilitates latecomer firms′ technological catch-up from the perspective of entrepreneurship. ***Journal of Management Science***, 2023, 36(2): 53−74.

[3] 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?. **管理世界**, 2021, 37(5): 170−190.
LIU Shuchun, YAN Jinchen, ZHANG Sixue, et al. Can corporate digital transformation promote input-output efficiency?. ***Journal of Management World***, 2021, 37(5): 170−190.

[4] 赵昕, 单晓文, 王垒. 数字化转型与企业脱虚向实. **管理科学**, 2023, 36(1): 76−89.
ZHAO Xin, SHAN Xiaowen, WANG Lei. Digital transformation and enterprises′ industrialization and definancialization. ***Journal of Management Science***, 2023, 36(1): 76−89.

[5] LI H, YOO S, KETTINGER W J. The roles of IT strategies and security investments in reducing organizational security breaches. ***Journal of Management Information Systems***, 2021, 38(1): 222−245.

[6] SKRYNNYK O. Some aspects of information security in digital organizational management system. ***Marketing and Management of Innovations***, 2020(4): 279−289.

[7] ALGHAMDI S, THAN W K, VLAHU-GJORGIEVSKA E. Information security governance challenges and critical success factors: systematic review. ***Computers & Security***, 2020, 99: 102030-1−102030-39.

[8] DONG J Q, KARHADE P P, RAI A, et al. How firms make information technology investment decisions: toward a behavioral agency theory. ***Journal of Management Information Systems***, 2021, 38(1): 29−58.

[9] SAFI R, BROWNE G J, NAINI A J. Mis-spending on information security measures: theory and experimental evidence. ***International Journal of Information Management***, 2021, 57: 102291-1−102291-14.

[10] HAISLIP J, LIM J H, PINSKER R. The impact of executives′ IT expertise on reported data security breaches. ***Information Systems Research***, 2021, 32(2): 318−334.

[11] GONZALEZ P A, ASHWORTH L, MCKEEN J. The CIO stereotype: content, bias, and impact. ***The Journal of Strategic Information Systems***, 2019, 28(1): 83−99.

[12] MIRTSCH M, BLIND K, KOCH C, et al. Information security management in ICT and non-ICT sector companies: a preventive innovation perspective. ***Computers & Security***, 2021, 109: 102383-1−102383-23.

[13] HADLINGTON L, BINDER J, STANULEWICZ N. Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. ***Computers in Human Behavior***, 2021, 114: 106557-1−106557-8.

[14] 甄杰, 谢宗晓, 董坤祥. 信息安全压力与员工违规意愿: 被调节的中介效应. **管理科学**, 2018, 31(4): 91−102.
ZHEN Jie, XIE Zongxiao, DONG Kunxiang. Information security stress and employees′ violation intention: moderated mediation effects. ***Journal of Management Science***, 2018, 31(4): 91−102.

[15] 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. **南开管理评论**, 2020, 23(1): 158−168.
ZHEN Jie, XIE Zongxiao, LI Kanghong, et al. Information security governance and firm performance: a moderated mediation effect model. ***Nankai Business Review***, 2020, 23(1): 158−168.

[16] 周昊, 李俊, 王冲华, 等. 工业互联网安全公共服务能力提升路径研究. **中国工程科学**, 2021, 23(2): 74−80.
ZHOU Hao, LI Jun, WANG Chonghua, et al. Paths for improving public service capability regarding industrial internet security. ***Strategic Study of CAE***, 2021, 23(2): 74−80.

[17] TEUBNER R A, STOCKHINGER J. Literature review: understanding information systems strategy in the digital age. ***The Journal of Strategic Information Systems***, 2020, 29(4): 101642-1−101642-28.

[18] SCHLACKL F, LINK N, HOEHLE H. Antecedents and con-

sequences of data breaches: a systematic review. ***Information & Management***, 2022, 59(4): 103638-1−103638-15.

[19] WESSEL L, BAIYERE A, OLOGEANU-TADDEI R, et al. Unpacking the difference between digital transformation and IT-enabled organizational transformation. ***Journal of the Association for Information Systems***, 2021, 22(1): 102−129.

[20] 徐二明, 肖建强. 战略管理研究的演进. **管理科学**, 2021, 34(4): 101−114.
XU Erming, XIAO Jianqiang. Evolution of strategic management research. ***Journal of Management Science***, 2021, 34(4): 101−114.

[21] YANG J J, ZHANG F, JIANG X, et al. Strategic flexibility, green management, and firm competitiveness in an emerging economy. ***Technological Forecasting and Social Change***, 2015, 101: 347−356.

[22] 孙璐, 李力, 孔英. 信息交互能力的测度及其对竞争优势的影响研究: 基于用户体验的价值共创视角. **管理工程学报**, 2018, 32(2): 67−83.
SUN Lu, LI Li, KONG Ying. Measurement of information interaction capacities and its impact on competitive advantage: from the perspective of value co-creation. ***Journal of Industrial Engineering/Engineering Management***, 2018, 32(2): 67−83.

[23] 张琳, 席酉民, 杨敏. 资源基础理论60年: 国外研究脉络与热点演变. **经济管理**, 2021, 43(9): 189−208.
ZHANG Lin, XI Youmin, YANG Min. Resource based theory in 60 years: international theoretical development and hotspots evolution. ***Business and Management Journal***, 2021, 43(9): 189−208.

[24] 张璐, 王岩, 苏敬勤, 等. 资源基础理论: 发展脉络、知识框架与展望. **南开管理评论**, 2023, 26(4): 246−256.
ZHANG Lu, WANG Yan, SU Jingqin, et al. Resource-based theory: development context, knowledge framework and outlook. ***Nankai Business Review***, 2023, 26(4): 246−256.

[25] 甄杰, 谢宗晓, 林润辉. 治理机制、制度化与企业信息安全绩效. **工业工程与管理**, 2018, 23(3): 171−176, 191.
ZHEN Jie, XIE Zongxiao, LIN Runhui. Governance mechanism, institutionalization, and enterprises′ information security performance. ***Industrial Engineering and Management***, 2018, 23(3): 171−176, 191.

[26] 吕孝礼, 付帅泽, 朱宪, 等. 突发事件协同研判行为研究: 研究进展与关键科学问题. **中国科学基金**, 2020, 34(6): 693−702.
LYU Xiaoli, FU Shuaize, ZHU Xian, et al. Joint crisis sensemaking: a review and research agenda. ***Bulletin of National Natural Science Foundation of China***, 2020, 34(6): 693−702.

[27] 甄杰, 谢宗晓, 林润辉. 企业信息安全制度化部署过程的行动研究. **管理案例研究与评论**, 2018, 11(2): 192−209.
ZHEN Jie, XIE Zongxiao, LIN Runhui. Action research on the institutionalization implementation of enterprises′ information security. ***Journal of Management Case Studies***, 2018, 11(2): 192−209.

[28] DEANE J K, GOLDBERG D M, RAKES T R, et al. The effect of information security certification announcements on the market value of the firm. ***Information Technology and Management***, 2019, 20(3): 107−121.

[29] YOON J, KIM Y, VONORTAS N S, et al. Corporate foresight and innovation: the effects of integrative capabilities and organisational learning. ***Technology Analysis & Strategic Management***, 2018, 30(6): 633−645.

[30] PANG C W, WANG Q, LI Y, et al. Integrative capability, business model innovation and performance: contingent effect of business strategy. ***European Journal of Innovation Management***, 2019, 22(3): 541−561.

[31] 韩自强. 应急管理能力: 多层次结构与发展路径. **中国行政管理**, 2020(3): 137−142.
HAN Ziqiang. A multi-level framework of developing emergency management capacities. ***Chinese Public Administration***, 2020(3): 137−142.

[32] 尹佳音. 美、日、印构建信息安全体系的思路与借鉴. **宏观经济管理**, 2021(4): 84−90.
YIN Jiayin. The thinking on and inspiration from the information security systems of the United States, Japan and India. ***Macroeconomic Management***, 2021(4): 84−90.

[33] 李维安, 张耀伟, 孟乾坤. 突发疫情下应急治理的紧迫问题及其对策建议. **中国科学院院刊**, 2020, 35(3): 235−239.
LI Weian, ZHANG Yaowei, MENG Qiankun. Urgent problems and countermeasures of emergency governance system under COVID-19 outbreak. ***Bulletin of Chinese Academy of Sciences***, 2020, 35(3): 235−239.

[34] 池毛毛, 叶丁菱, 王俊晶, 等. 我国中小制造企业如何提升新产品开发绩效: 基于数字化赋能的视角. **南开管理评论**, 2020, 23(3): 63−75.
CHI Maomao, YE Dingling, WANG Junjing, et al. How can Chinese small-and medium-sized manufacturing enterprises improve the new product development (NPD) performance? From the perspective of digital empowerment. ***Nankai Business Review***, 2020, 23(3): 63−75.

[35] ZHEN J, XIE Z X, DONG K X. Impact of IT governance mechanisms on organizational agility and the role of top management support and IT ambidexterity. ***International Journal of Accounting Information Systems***, 2021, 40: 100501-1−100501-15.

[36] 谢智敏, 王霞, 杜运周, 等. 创业生态系统如何促进城市创业质量: 基于模糊集定性比较分析. **科学学与科学技术管理**, 2020, 41(11): 68−82.
XIE Zhimin, WANG Xia, DU Yunzhou, et al. How does the entrepreneurial ecosystem promote urban entrepreneurial quality? A fuzzy set qualitative comparative analysis. ***Science of Science and Management of S.&T.***, 2020, 41(11): 68−82.

[37] ZHANG Y Y, ZHANG C, XU Y J. Effect of data privacy and security investment on the value of big data firms. ***Decision Support Systems***, 2021, 146: 113543-1−113543-12.

[38] 吴松强, 蔡婷婷, 赵顺龙. 产业集群网络结构特征、知识搜索与企业竞争优势. **科学学研究**, 2018, 36(7): 1196−1205, 1283.
WU Songqiang, CAI Tingting, ZHAO Shunlong. Industrial cluster network structure characteristic, knowledge search and enterprise′s competitive advantage. ***Studies in Science of Science***, 2018, 36(7): 1196−1205, 1283.

[39] 肖勰, 卢晓, 芮明杰. 企业遗产对持续竞争优势的影响研究: 品牌资产的中介作用和动态能力的调节作用. **南开管理评论**, 2019, 22(2): 155−164.
XIAO Xie, LU Xiao, RUI Mingjie. A study of the influence of corporate heritage on sustainable competitive advantage: brand assets and the moderating effect of dynamic capability. ***Nankai Business Review***, 2019, 22(2): 155−164.

[40] PRASAD A, GREEN P, HEALES J. On IT governance structures and their effectiveness in collaborative organizational structures.

International Journal of Accounting Information Systems, 2012, 13(3): 199−220.

[41] 刘天畅, 李向阳, 于峰. 案例驱动的 CI 系统应急能力不足评估方法. **系统管理学报**, 2017, 26(3): 464−472.
LIU Tianchang, LI Xiangyang, YU Feng. Case-driven assessment method for emergency capability shortage of critical infrastructure system. ***Journal of Systems & Management***, 2017, 26(3): 464−472.

[42] 张吉军, 姜一, 申婧. 企业突发事件应急能力形成机理探析. **中国安全生产科学技术**, 2014, 10(10): 160−165.
ZHANG Jijun, JIANG Yi, SHEN Jing. Study on formation mechanism of emergency response capability in enterprise. *Journal of Safety Science and Technology*, 2014, 10(10): 160−165.

[43] LIANG H G, SARAF N, HU Q, et al. Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, 2007, 31(1): 59−87.

[44] 温忠麟, 叶宝娟. 中介效应分析: 方法和模型发展. **心理科学进展**, 2014, 22(5): 731−745.
WEN Zhonglin, YE Baojuan. Analyses of mediating effects: the development of methods and models. *Advances in Psychological Science*, 2014, 22(5): 731−745.

[45] 杜运周, 贾良定. 组态视角与定性比较分析 (QCA): 管理学研究的一条新道路. **管理世界**, 2017, 33(6): 155−167.
DU Yunzhou, JIA Liangding. Configurational perspective and qualitative comparative analysis (QCA): a new approach to management research. *Journal of Management World*, 2017, 33(6): 155−167.

[46] 徐广平, 张金山, 杜运周. 环境与组织因素组态效应对公司创业的影响: 一项模糊集的定性比较分析. **外国经济与管理**, 2020, 42(1): 3−16.
XU Guangping, ZHANG Jinshan, DU Yunzhou. The impact of environmental and organizational configuration on corporate entrepreneurship: a fuzzy-set qualitative comparative analysis. ***Foreign Economics & Management***, 2020, 42(1): 3−16.

[47] 程建青, 罗瑾琏, 杜运周, 等. 何种创业生态系统产生女性高创业活跃度?. **科学学研究**, 2021, 39(4): 695−702.
CHENG Jianqing, LUO Jinlian, DU Yunzhou, et al. What kinds of entrepreneurial ecosystem can produce country-level female high entrepreneurial activity?. *Studies in Science of Science*, 2021, 39(4): 695−702.

[48] DHILLON G, SMITH K, DISSANAYAKA I. Information systems security research agenda: exploring the gap between research and practice. ***The Journal of Strategic Information Systems***, 2021, 30(4): 101693-1−101693-17.

[49] 陈晓红, 周艳菊, 徐选华, 等. 突发公共卫生事件下的应急运作管理研究. **管理科学**, 2022, 35(1): 42−49.
CHEN Xiaohong, ZHOU Yanju, XU Xuanhua, et al. On emergency operation management under public health emergency. *Journal of Management Science*, 2022, 35(1): 42−49.

The Impact of Information Security Collaborative Governance on Enterprise Competitive Advantages in the Process of Digital Transformation

ZHEN Jie[1], XIE Zongxiao[2], DONG Kunxiang[3], LIN Runhui[4]

1 School of Management Science and Engineering, Chongqing Technology and Business University, Chongqing 400067, China

2 Legal and Compliance Department, China Financial Certification Authority, Beijing 100054, China

3 School of Management Science and Engineering, Shandong University of Finance and Economics, Jinan 250014, China

4 Business School, Nankai University, Tianjin 300071, China

Abstract: Digital transformation is the path for enterprises to better perceive and meet external market demands, as well as to realize and refine internal digital operation management. However, frequent information security incidents such as data leakage during the digital transformation which not only cause serious losses to enterprises, but also endanger the national security and social stability. This situation also shows that information security governance in enterprise digital transformation lags far behind the real needs. So far, the existing studies have not paid enough attention to information security issues in enterprise digital transformation.

Based on the resource-based theory, this study explores the impact of information security collaborative governance on the competitive advantage of enterprises in digital transformation from the value creation function of information security. Furthermore, this study explores the mediating roles of information security integrative capability and emergency capability. As such, we can verify the theoretical logic of “information security governance-information security capability-value creation”. The

hypotheses are tested by using structural equation modeling (SEM) and fuzzy set qualitative comparative analysis (fsQCA) with data from 136 domestic enterprises promoting digital transformation.

The results show that, (1) Information security collaborative governance, information security integrative capability and information security emergency capability have significant positive effects on enterprise competitive advantage, respectively. In addition, these three variables form two types of antecedent constructs of enterprise competitive advantage; (2) Information security integrative capability and information security emergency capability play partly mediating roles in the relationship between information security collaborative governance and enterprise competitive advantage; (3) In comparison, the impact of information security integrative capability on enterprise competitive advantage is greater than that of information security emergency capability. However the complementary effect of these two variables is not significant.

The results clarify the rationality of the theoretical logic that "information security governance-information security capability-value creation", confirm the positive impact of information security collaborative governance on enterprise competitive advantage in digital transformation, and expand the theoretical understanding of the impact of information security integrative capability, information security emergency capability. The theoretical cognition of the impact of information security integration capability and information security emergency capability is expanded. Furthermore, suggestions regarding promoting information security collaborative governance, improving information security integrative capability and emergency capability provide practical support for enterprises to reasonably and effectively control information security risks in digital transformation.

Keywords: digital transformation; information security collaborative governance; information security integrative capability; information security emergency capability; competitive advantages

Received Date: July 12th, 2022 **Accepted Date:** January 31st, 2024

Funded Project: Supported by the National Natural Science Foundation of China (72102025), the National Social Science Fund of China (21CGL017), the Chongqing Social Science Planning Project (2021NDYB083), and the Chongqing Municipal Education Commission Scientific and Technological Research Project (KJQN202100842)

Biography: ZHEN Jie, doctor in management, is an associate professor in the School of Management Science and Engineering at Chongqing Technology and Business University. His research interests include information security governance and corporate digital transformation. His representative paper titled "Information security governance and firm performance: a moderated mediation model" was published in the ***Nankai Business Review*** (Issue 1, 2020). E-mail: zhenjie@vip.126.com

XIE Zongxiao, doctor in management, is a deputy researcher in the Legal and Compliance department at China Financial Certification Center. His research interest focuses on network and information security management. E-mail: xiezongxiao@vip.163.com

DONG Kunxiang, doctor in management, is an associate professor in the School of Management Science and Engineering at Shandong University of Finance and Economics. His research interest focuses on cyber security insurance. His representative paper titled "Optimal decision analysis of information security investment and cyber insurance under mandatory constraints" was published in the ***Chinese Journal of Management Science*** (Issue 6, 2021). E-mail: dkxgood@163.com

LIN Runhui, doctor in management, is a professor in the Business School at Nankai University. His research interest focuses on information security governance. E-mail: linrh@nankai.edu.cn □

(责任编辑：李祎博)