

基于大数据安全视角的管理实践研究

蒋志强¹

澳门科技大学商学院, 中国澳门, 999078

西南医科大学, 中国泸州, 646000

摘要: 数字经济时代, 大数据已成为企业战略转型和持续竞争优势的关键驱动力。在技术创新和监管合规的双重压力下, 企业必须妥善处理数据利用与数据安全之间的矛盾。本研究从大数据安全治理的视角, 探讨了中国领先的数字化解决方案提供商凌阳智能的管理实践。研究以资源基础观(RBV)为基础, 识别瓴羊智能独有且不可复制的资源, 包括自有数据资产、人工智能驱动的平台和治理机制, 并分析如何通过全生命周期数据安全治理、行业解决方案设计以及平台级创新等结构化流程, 将这些资源转化为组织能力。本研究在理论上将资源基础观扩展到中国的数字治理领域, 在实践上为其他企业在数据驱动创新和网络安全合规的双重要求下提供可复制的参考模型。此外, 本研究还为监管机构在统一评估指标、人才培养和国家数据战略协调等方面提出了政策建议。

关键词: 大数据安全; 资源基础观(RBV); 数字治理; 战略管理

一、研究背景

随着数字经济时代的到来, 大数据成为驱动企业战略转型和核心竞争力构建的重要资产。中国在推动数字中国、网络强国的战略背景下, 企业数字化转型步伐显著加快, 同时也面临着前所未有的大数据安全挑战。大数据时代各国政府均十分重视数据安全治理出台的相关档已成为各行业制定数据安全规范的主要参考标准。美国国家标准与技术研究院(National Institute of Standards and Technology, 简称NIST)制定了《NIST 大数据互操作性框架》, 从定义、操作、安全及隐私等方面探讨数据安全控制管理的具体内容。我国为加速推进大数据安全标准研究与管理, 国家信息安全标准化技术委员会相继发布了《大数据安全标准化白皮书》2017、2018版, 2019年制定的《信息安全技术大数据安全管理指南》(GB/T37973-2019)从大数据安全需求、大数据安全要求、大数据安全风险等角度勾画我国大数据安全管理整体轮廓, 以供各类组织展开数据安全治理或评估参考。

近年来, 大数据安全问题在学术界也引发了大量的思考和讨论, 数据安全的当务之急是数据技术领域的热点问题, 它的核心内容是保护用户的隐私、完整性、可用性等。保证数据不会为非授权人员和机构访问, 对于维护个人隐私权和企业商业机密至关重要(赵劲强, 等 2024; Tao H, et al 2018)。互联网、电信、金融、医疗、政府等不同行业组织均有不同程度的大数据安全需求, 主要涉及数据保密、隐私保护、数据的产生、存储和分析等系列安全问题(胡坤、刘镒、刘明辉, 2014; Eling M., Wirfs J., 2019)。金融业存在的大大数据安全问题为隐私泄露风险过大、防御技术不当以及平台安全防护欠缺, 解决这些大数据安全问题可以通过数据安全防范技术、数据分析技术、隐私保护技术等策略(唐彬、吴晓光, 2017; Tao H, et al, 2018)。鉴于企业的市场主体作用, 众多学者围绕企业大数据应用及安全问题展开研究, 指出数据管理是企业、行业或政府成功的关键。大数据是企业创造价值的重要工具, 也是实现企业可持续发展的重要因素, 可通过保护客户数据安全、数据安全共享等方式加强企业和顾客之间的信任(Rehman, et al, 2016)。此外, 大数据对企业的战略决策、运营管理及商业模式也都产生巨大影响。大数据时代企业需要进行大数据治理, 具体指大数据风险管理、价值管理及成本管理(Tallon, 2013; Mounir El Khatib et al,

¹ 作者简介: 蒋志强, 四川资阳人, 澳门科技大学工商管理硕士, 博士生, 西南医科大学, 研究方向为: 组织行为学、医学人文教育、领导力等。email:jiangzhiqiang1988@163.com。

2023)。研究表明安全技术策略只是解决企业大数据安全问题的基础,为发挥技术策略的最大效益,企业需要制定相应的大数据安全策略(刘力钢、刘建基,2016; Abdelhalim AM, Hassan M, 2025)。综合上述观点,保护企业大数据安全须是安全技术与安全管理双管齐下、相得益彰。瓴羊公司作为中国领先的数字化解决方案提供商,专注于大数据平台建设与行业智能化升级,在国家政策导向与市场需求推动下迅速崛起。在数字化治理深入推进过程中,企业如何平衡数据创新与安全合规、如何通过科学管理提升组织韧性与数据治理能力,成为理论研究与实践探索的双重命题。基于此,本文拟从管理学经典理论出发——资源基础观(Resource-Based View, RBV),深入剖析瓴羊公司在大数据安全治理、数据资产运营、技术赋能产业升级等方面的管理实践,以期为中国企业在数字时代的可持续发展提供理论支持与实践范式。

二、研究目的与意义

数据安全贯穿数据采集、存储、处理、分析、销毁整个数据生命周期,为深入了解企业大数据安全,结合大数据安全及大数据特征,企业大数据安全涉及的要素可归纳为大数据技术、大数据管理和大数据应用3个维度,技术与管理是大数据安全体系内相辅相成的有机组成部分,因此企业大数据安全建设中,以大数据技术为基础策略,大数据管理为机制屏障,大数据应用为终极目标,三维要素紧密关联、相互支撑。探究瓴羊公司如何将资源优势转化为大数据治理能力,验证RBV在中国数字企业中的适用性与边界;分析、总结瓴羊公司在数据安全治理、跨行业赋能与组织转型等方面的实践经验,提炼适合中国情境的管理模型为数字经济下中国企业的管理创新与数据治理体系建设提供借鉴与参考。

三、公司概况

公司简介:瓴羊公司(Lingyang Intelligence)隶属于阿里云体系,是国内领先的企业数据智能平台服务提供商。公司聚焦“让数据更普惠,让商业更智能”,业务涵盖一站式数据中台搭建、行业数据解决方案、AI算法模型训练、数据安全治理等领域,服务对象涵盖政府、金融、制造、零售等多个行业(宋婧,2023)。涵盖数据加工、数据消费以及数据流通等三大环节。帮助企业有效利用数据资源,促进数据与企业实际运营的深度融合,赋能企业增长和数字化转型。截至2024年9月,瓴羊已服务超过5万家企业、遍布20个行业,例如服务了超20家乳业品牌和超70家汽车品牌,如一汽红旗、伊利、蒙牛、极氪、中国移动和中海油等,覆盖零售、汽车与制造、互联网、金融等多个行业。

1. 产品矩阵

企业数据加工:Dataphin智能数据建设与治理,Quick BI数据可视化分析;企业数据消费:Quick Audience全管道消费者运营增长,Quick Service全触点智能服务管理;行业数据流通:瓴羊港——企业数据服务枢纽。

2. 主要产品与服务

数据中台解决方案:帮助客户构建稳定、可复用的数据资源体系;智能决策平台:通过AI分析助力业务预测、流程优化;安全合规体系:提供数据脱敏、权限管理、安全审计等功能,确保数据合法合规使用;行业解决方案:包括智慧政务、智能制造、数字零售等。

3. 战略定位与市场优势

强大的生态资源依托阿里云,具备平台、技术、数据和人才多重优势具备自主研发能力,数据治理工具链和AI引擎成熟;积极回应国家政策,在信创产业链布局与国产替代中发挥重要作用。

四、基于资源基础观(RBV)的分析

根据企业的资源基础观(RBV),企业拥有宝贵的、稀缺的、竞争对手难以复制的资源 and 能力(Yu et al., 2018)。在RBV观点中,能力是指企业利用资源“实现期望目标”的能力,相当于企业通过组织流程生产的中间商品,以实现“更高的资源效率”(Yu et al., 2018)。研究人

员采用与 RBV 类似的理论来研究企业内部的资源和能力,即:动态能力观(DCV)和权变理论(CT)。DCV 是应对不确定性时观察资源的最有利的视角,而权变理论则应用于领导力理论。然而,本调研的是瓴羊在大数据驱动的 VRIN 资源;因此,采用 RBV,因为根据 Kumar et al. (2023) 的研究,企业资源价值观的核心理论是将企业视为实现 CA 所需的一系列有价值的有形和无形资源(Kumar et al., 2023)。它将这些资源描述为企业特有的、稀缺的、独特的和准资源,并将其视为帮助企业实施价值创造战略以获取利润的手段(Kumar et al., 2023)。在资源价值观中,可以区分资源选择和能力发展,这是资源价值观的两个独立方面。寻找、采购或管理具有战略价值的资源的行为称为资源挑选,而能力建设则侧重于协调和利用现有资源以创造潜在的可用资产(Mikalef et al., 2018)。

1. 关键资源识别

根据 RBV 理论,企业竞争优势来源于稀缺、不可模仿、难替代的资源。瓴羊的关键资源包括:

- (1) 数据资源:海量行业数据积累,涵盖政务、金融、零售等场景;
- (2) 技术资源:拥有自主研发的数据中台产品和 AI 建模平台;
- (3) 人力资本:核心团队来自阿里系,具备丰富的互联网和技术背景;
- (4) 组织制度与流程:形成一套标准化、安全合规、可复制的解决方案体系。

2. 资源转化为能力路径

瓴羊通过资源整合与协同创新,构建大数据安全治理能力:

- (1) 数据安全治理:构建数据生命周期管理制度,实现从采集、传输、存储、处理到销毁的全流程安全管控;
- (2) 客户定制能力:根据不同行业需求定制解决方案,实现资源向客户价值的转化;
- (3) 动态适应能力:通过平台架构灵活性与模块化设计,应对政策与市场变化。

3. 资源可持续性分析

由于技术和行业知识具有累积性,瓴羊的资源基础具备持续优化能力;但其也面临高端人才流动、技术快速更迭等外部不确定性,需要持续投资与组织变革以维系竞争优势。

五、大数据安全视角下的管理挑战与应对

1. 主要挑战

- (1) 合规风险:面对多重法规交叉(如数据出境、行业标准)需要加强法律合规审查;
- (2) 内部治理:数据使用权责不清、数据孤岛问题影响资源整合;
- (3) 技术安全:面临恶意攻击、算法安全、模型偏见等新型风险;
- (4) 客户信任:企业客户对数据安全信任不足,影响合作深度。

2. 应对策略

- (1) 制度建设:建立内部数据安全委员会,统一管理制度与流程;
- (2) 技术防线:部署多重加密、零信任架构、AI 安全识别等前沿技术;
- (3) 员工赋能:开展安全意识培训,提升员工对数据资产重要性的认识;
- (4) 对外合作:与政府机构、科研院所合作参与标准制定与安全框架研发

六、管理启示与未来建议

1. 瓴羊公司在大数据安全领域的的能力画像(SWOT)分析

优势(S): 阿里云生态支撑,资源平台强大;- 技术能力领先,研发投入稳定;- 行业解决方案丰富,定制化程度高;- 数据安全治理制度完善,信任度高。

劣势(W): 高度依赖母公司技术平台,独立性仍有限;- 高端人才流动率较高;- 缺乏国际市场扩展经验。

机会(O)：国家政策支持数据安全与国产替代；- 各行业数字化转型需求上升；- 行业标准制定机会增多。

威胁(T)：华为、腾讯等强势竞争者快速推进；- 法规变化频繁，加重合规成本；- 客户对隐私和数据安全要求提升。

2.战略建议：构建可持续的竞争优势

(1) 差异化战略深化：强化行业知识沉淀，打造“行业+数据+合规”一体化解决方案矩阵；建议设立专门的行业智库团队，推动跨部门、跨行业协作平台发展。

(2) 人才与组织韧性建设：引入“数字治理+组织学习”双轨培训体系，构建学习型组织文化；提高员工参与感，设立内部创新激励机制，减少技术人才流失。

(3) 数据安全“全生命周期治理”策略：推动构建“预防-检测-回应-恢复”四位一体安全框架；强化AI在数据风险识别、用户行为审计、算法可信性等方面的实用化。

(4) 品牌与客户关系策略：建议强化“可信数据伙伴”品牌定位，输出更多标准化白皮书和案例；推行客户共创机制，将关键客户嵌入产品设计与反馈流程。

(5) 中长期海外市场探索：在“一带一路”沿线国家先行试点数据平台出海业务，增强抗风险能力；建议设立海外合规研究小组，为国际扩张提前准备制度与技术方案。

3.理论融合的重要性

瓴羊的实践表明，RBV与OLT的有机结合有助于实现资源价值最大化与组织持续创新：RBV帮助企业识别和积累核心资源，OLT则推动资源高效流动与价值实现；在大数据安全环境下，仅有资源优势不足，必须具备快速学习与适应能力。

4.对中国企业的启示

企业应构建数据资产视角下的战略管理体系，将数据纳入核心资源范畴；建议构建以学习型组织为导向的数字治理模式，强化组织适应性；加强跨部门协作与知识融合，打破“烟囱式”数据管理结构。

5.对政策制定者的建议

鼓励头部企业参与国家数据治理框架建设，输出实践经验；推动构建统一的数据安全评价指标体系，降低企业合规不确定性；支持数字安全人才培养，弥合企业在专业技术领域的人才短板。

七、结语

随着中国数字化进程不断加快，大数据安全已成为企业治理体系建设的关键组成部分。数字经济时代国家和企业都十分重视数据安全问题，企业大数据安全是一个复杂、动态的系统，也是一项极具挑战性的任务。建立大数据安全评价指标体系有助于企业集团及社会大众系统了解企业数据安全评价方向、为企业数据安全防御提供理论参考。首先在文献梳理的基础上界定大数据安全内涵，明确企业大数据安全的要素包括技术安全、管理安全及应用安全，及基于资源基础观和SWOT的分析。瓴羊公司的管理实践为我们提供了观察中国数字企业在资源管理、组织学习与数据治理融合过程中的典范。通过RBV视角，不仅加深了对企业战略行为的理解，也为探索中国特色数字治理模式提供了理论支持。未来，企业如何在保持安全合规的基础上实现价值创新，将成为决定其核心竞争力的关键。

参考文献

中文部分

王欣亮、任弢、刘飞：《基于精准治理的大数据安全治理体系创新》，《中国行政管理》，2019年(12):121-126。

宋婧、瓴羊 CEO 朋新宇：《智能化就是大模型加上好数据[N]》，《中国电子报》，2023-08-01(004).DOI:10.28065/n.cnki.ncdzb.2023.000998.

胡坤、刘镒、刘明辉：《大数据的安全理解及应对策略研究》，《电信科学》，2014，30(2):112-117,122。

唐彬、吴晓光：《金融业大数据安全问题》，《中国金融》，2017，(23):77-78。

周胜利、陈斌、吴礼发：《大数据环境下电信运营商数据安全保护方案》，《电信科学》，2017，33(5):119-125。

陈文捷、蔡立志：《大数据安全及其评估》，《计算机应用与软件》，2016，33(4):34-38。

叶晓俊、金涛、刘璘：《大数据安全标准现状和思考》，《科技导报》，2020，38(3):94-102。

孙红梅、贾瑞生：《大数据时代企业信息安全管理研究》，《科技管理研究》，2016，36(19):210-213。

赵劲强，楚栋，聂勤务：《大数据视域下计算机信息安全及防护的几点思考[J]》，《信息与计算机(理论版)》，2024，36(7):197-199。

刘力钢、刘建基：《大数据对企业竞争优势影响的理论与展望》，《管理现代化》2016，36(5):110-112。

刘勳钊：《大数据环境下企业信息安全管理构建》，《中外企业家》，2018，(6):45。

全国信息安全标准化技术委员会：《信息安全技术大数据安全管理指南[EB/OL]》，(2019-08-30)[2020-05-03].<https://www.tc260.org.cn/front/bzcx/yfgbcx.html>.

英文部分

Abdelhalim, A.M., Hassan, M.(2025).Exploring the impact of big data analytics and risk management convergence on sustainability performance development: an accounting perspective. *Discov Sustain*,6,175.

Chaudhuri S, Dayal U, Narasayya V.(2011).An overview of business intelligence technology.*Communications of the ACM*,54(8):88-98.

Eling M., Wirfs J. (2019).What are the actual costs of cyber risk events?*European J Oper Res*, 272 (3):1109-1119.

Kumar, M., Raut, R. D., Gunasekaran, A., Venkateshwarlu, M., & Choubey, V. K. (2023).Developing supply chain capabilities through digitalization and viability for controlling the ripple effect. *IEEE Transactions on Engineering Management*,1-17.

Mikalef, P., Pappas, I. O., Krogstie, J., & Giannakos, M.(2018). Big data analytics capabilities: A systematic literature review and research agenda.*Information Systems and e-Business Management*, 16, 547-578. <https://doi.org/10.1007/s10257-017-0362-y>.

NIST. Big data information [EB/OL] .(2015-09)[2020-04-27] .
<https://www.nist.gov/el/cyber-physical-systems/big-data-pwg>.

Tao H., Bhuiyan M.Z.A., Abdalla A., Hassan M., Jain J., Hayajneh T.(2018).Secured data collection with hardware-based ciphers for iot-based healthcare.*IEEE Internet Things J. (IEEE IoT-J)* ,1-10.

Tallon P P.(2013).Corporate governance of big data: *Perspectives on value, risk, and cost.Computer*, 46(6):32-38.

Ur Rehman M H, Chang V, Batool A, et al.(2016).Big data reduction framework for value creation in sustainable enterprise.*International journal of information management*,36(6):917-928.

Yu, W., Chavez, R., Jacob, M. A., & Feng, M. (2018).Data-driven supply chain capabilities and performance: A resource-based view. *Transportation Research Part E: Logistics and Transportation Review*, 114, 371–385.

Research on management practice based on the perspective of big data security
Zhiqing Jiang

Abstract: In the digital economy era, big data has become a key driver for corporate strategic transformation and sustainable competitive advantage. Under the dual pressure of technological innovation and regulatory compliance, enterprises must properly handle the contradiction between data utilization and data security. This study explores the management practices of Lingyang Intelligent Technology, a leading digital solution provider in China, from the perspective of big data security governance. Based on the resource-based view (RBV), the study identifies Lingyang Intelligent Technology's unique and non-replicable resources, including its data assets, artificial intelligence-driven platforms, and governance mechanisms. It analyzes how to transform these resources into organizational capabilities through structured processes such as full-life cycle data security management, industry solution design, and platform-level innovation. This study theoretically extends the resource-based view to China's digital governance field, and in practice, provides a replicable reference model for other companies under the dual requirements of data-driven innovation and cybersecurity compliance. In addition, this study also presents policy recommendations for regulators, focusing on unified evaluation indicators, talent training, and national data strategy coordination.

Keywords: Big data security; Resource-based view (RBV); Digital governance; Strategic management