

企业数字化转型中的信息安全管理同步推动

许珊珊

中国石化销售股份有限公司湖北石油分公司, 中国·湖北 武汉 430030

摘要: 为提高企业信息安全管理水平, 选择某某上市公司, 分析其在 2015—2024 年之间的数据, 提出三点假设。经过统计学分析与验证, 确定企业数字化转型、信息安全管理、声誉、人力资源之间具有密切的联系, 并且能够推动企业的数字化转型。基于此结论, 提出构建网络安全网络、建设信息等级化管理制度、定期升级维护信息安全管理信息系统三点建议, 希望能为今后企业数字化转型以及信息安全管理提供一定程度的借鉴。

关键词: 企业; 数字化转型; 信息安全管理; 同步推动

Simultaneous Promotion of Information Security Management in Enterprise Digital Transformation

Shanshan Xu

Sinopec Sales Co., Ltd. Hubei Petroleum Branch, Wuhan, Hubei, 430030, China

Abstract: To enhance the level of enterprise information security management, a certain listed company was selected, and its data from 2015 to 2024 was analyzed to propose three hypotheses. Through statistical analysis and verification, it was determined that there is a close relationship between the company's digital transformation, information security management, reputation, and human resources, which can promote the company's digital transformation. Based on this conclusion, three suggestions were put forward: constructing a network security network, establishing an information classification management system, and regularly upgrading and maintaining the information security management system. It is hoped that these suggestions can provide some reference for future digital transformation and information security management of enterprises.

Keywords: enterprise; digital transformation; information security management; simultaneous promotion

0 前言

企业生产经营在大数据、物联网、人工智能等技术的推动下, 逐渐实现了生产制造模式的升级, 而且企业内部资金、人才和物资等信息链也得到整合, 打破了多项因素造成的限制, 切实增强了企业内部资源分配的合理性, 提高了效率。企业数字化转型中面临信息安全隐患, 这也是注册信息安全管理人员, 即 ciso 的重要工作内容。一旦大量数据整合, 势必催生多种业态, 形成新的经济增长点, 企业方面考虑到降本增效的需求, 在数字化转型中开发一些新的路径, 面向企业中的重要机密数据, 如人力资源数据、财务数据和研发数据等, 对其进行强有力的安全保护, 以免出现信息泄露的情况, 导致无可挽回的损失。有鉴于此, 论文以企业数字化转型下的信息安全管理为对象展开分析, 验证二者之间的必然联系。

1 理论基础与提出假设

1.1 信息安全管理与企业数字化转型的关联

综合当前与企业数字化转型相关的相关文献资料和研究成果, 多是关于企业产业改革与转型、资源分配与供给等, 将信息安全管理作为切入点的研究比较少^[1]。此次调查与研究检索资料发现, 部分学者将信息安全风险管理作为关注点, 以制度理论为基础展开分析。例如, 美国对信息安全相

关法律进行了完善, 划分不同类别, 分别阐述现行法律的执行对信息安全产生的积极影响与实践效果; 中国现行制度推动信息安全合法化的实践中, 是否形成了完善的作用机制。即便如此, 信息安全管理与企业数字化转型是否有直接的联系仍然需要深入探索^[2]。

结合企业信息安全管理现状, 发现制度的构建很少会对信息安全投资激励给予重视, 而且关于计算机犯罪惩处的内容也比较少, 代表企业仍然面临信息泄露风险, 也因为如此引起企业对信息安全问题的重视, 在该领域以及相关工作中增加投入, 只是关于二者之间的联系可参考与借鉴的研究成果有限^[3]。分析过程中发现 ISO27001 标准(即“信息安全要求 ISO/IEC27001”)是众多企业构建信息安全管理的重要参考, 也作为制度建设、完善可参考的规范发挥作用, 能对企业信息安全管理行为产生直观影响。所以, 信息安全管理可以采取构建认证体系的方式建设规范制度, 并且从理论层面推动企业数字化转型。由此提出假设:

假设 1: 信息安全管理能积极推动企业数字化转型。

1.2 信息安全管理、声誉和企业数字化转型的关联

企业在信息化时代下的数字化转型, 基于原有风险还增加了网络风险, 这也直接关系到企业的声誉。从信息安全角度分析网络风险, 主要是指企业接受委托后掌握个人数据泄露, 或者被黑客攻击, 导致企业本身以及利益相关者面临

声誉方面的损失，这对于企业而言，也会产生严重的消极影响，由此也肯定了网络风险防范在信息安全管理中的重要性，能维护企业的声誉^[4]。

参考 ISO27001 标准认证，其中提出了关于信息安全管理认证标准，一方面能帮助企业规避因行为规范性问题导致的网络风险，另一方面也可以防御黑客的恶意攻击，继而提升企业声誉。声誉是企业必需的无形资产，能持续性的创造价值，具有独特性和不可代替性^[5]。换言之，如果企业声誉具有较高的价值，代表可以利用声誉价值获取外部资源以及竞争的机会，推动企业转型与升级。从企业数字化转型的角度分析，除了对技术创新有较高的依赖性，还需要企业持续的投入资金^[6]。所以，企业声誉能间接推动企业数字化转型。基于此提出假设：

假设 2：信息安全管理可以获得声誉，继而推动企业数字化转型。

1.3 信息安全管理、人力资源和企业数字化转型的关联

企业受市场机制的影响，凭借技术偏向与资本深化，能对劳动弹性产生直观的影响，这种影响也体现在企业的劳动力收入上。如果劳动力资源比较少，势必会增加劳动要素价格，降低替代弹性^[7]。当技术水平提升且资本不断深化，

有利于实现资本偏向型的技术创新。由此分析，信息安全管理的实践中，构建规范性强的管理体能减少低端重复劳动力，从而获得更为可观的资本替代劳动。由此能够确定的一点是，信息安全管理作为企业数字化转型的一种新制度规范，能增加企业对技术型劳动力资源的需求，与之相对应的高技能劳动力价格也会随之升高，并会因此改变劳动收入分配^[8]。将其引申到信息安全管理工作中，可以在企业内部构建制度规范防御网络风险，并提高企业的竞争力。同理，企业人力资源结构发生变化，也能加快数字化转型的步伐。由此提出假设：

假设 3：信息安全管理以调整人力资源结构为措施，能推动企业数字化转型。

2 构建模型

2.1 数据来源

为验证以上提出假设，论文选择某上市公司在 2015—2024 年之间的数据作为分析对象，所有企业年报数据由北京证券交易所网站提供，地区经济增长的目标数据则是根据当地政府发布的工作报告提取，企业财务数据为官方发布。

2.2 设置变量

论文设置分析变量包括被解释变量、解释变量、控制变量等，具体关于各个变量定义如表 1 所示。

表 1 变量定义

变量项目	具体指标	代号	备注
被解释变量	企业数字化转型	Digital	—
解释变量	信息安全管理	ISO27001	企业已通过了信息安全管理体系认证，即 ISO27001=1，未通过认证为 ISO27001=0
控制变量	前十大股东持股比例	CR10	—
	审计意见	Audit	—
	企业规模	Asset	—
	资产负债率	Debt	—
	资产收益率	ROA	—
	净资产增长率	Netasset	—
	营业收入	Income	—
	企业净利润	Profit	—

2.3 建模

为验证论文提出假设，构建模型如下：

$$Digital_{it} = \alpha + \beta_1 ISO27001_{it-1} + \sum_{m=2} \beta_m Control_{it} + \sum year + \sum Ind + \sum Pro + \sum Firm + \varepsilon_{it} \quad (1)$$

模型中除了基本变量，Control 代表的是前述控制变量， ε 则代表了模型中的随机误差项。鉴于企业构建信息安全管理体系认证在推动数字化转型的实践中，可能有时滞情况，所以此次分析中对于设置的所有核心解释变量，均展开前置一期处理。同时，以免出现个体差异或面临时间、行业以及地区等多重差异，构建模型中还包含 Firm、Year、Ind、

Pro，依次对应的是个体固定效应、时间固定效应、行业固定效应、地区固定效应。

3 实证分析与检验

3.1 描述性统计

按照表 2 中统计的变量描述性数值，Digital 平均值是 0.7768，属于 0~11.5714 这一数值范畴，所以选定的样本中超过半数企业均已经走上了数字化转型道路，只是每家企业收获效果不同。表 2 中的 ISO27001 平均值是 0.0223，代表选择样本企业开展信息安全管理的比例只有 2.23%，可见数字化转型企业已经通过了信息安全管理体系认证的数量不多，即企业数字化转型与信息安全管理存在脱节的情况。

表 2 描述性统计结果

变量	样本数量	平均值	标准差	最大值	最小值
Digital	36010	0.7768	1.8253	11.5801	0.0000
ISO27001	37602	0.0223	0.1573	1.0000	0.0000
CR10	36148	60.0124	16.0710	98.0650	23.4507
Audit	35997	0.0182	0.1334	1.0000	0.0000
Asset	36352	17.4538	4.8052	25.5931	10.3923
Debt	37261	42.6752	21.5233	92.7522	5.0039
ROA	36358	6.4225	6.9902	28.7825	-19.4536
Netasset	36287	4.9326	3.3114	19.0420	0.3055
Income	36334	16.7859	4.8679	9.3578	25.1006
Profit	33851	0.4623	1.5987	5.1958	-3.2586
ET	36685	7.6002	2.1037	13.0000	0.0000

3.2 基准回归分析

企业数字化转型和信息安全管理进行基准回归分析，结果如表 3 所示。对个体固定效应进行控制，表 3 中列 (1) 的控制对象只是年份固定效应，计算得到 L.ISO27001 的回归系数为 2.1298，由此可知信息安全管理对于企业数字化转型具有促进作用。表 3 中的列 (2) 控制对象是行业固定效应，得到回归系数是 2.2564。表 3 中列 (3) 只是对地区固定效应进行控制，计算回归系数是 2.2661。表 3 中列 (4) 同时控制年份、行业、地区三项固定效应，回归系数是 2.1130，且以上所得回归系数均在 1% 水平显著为正，对比列 (1)、列 (2)、列 (3) 计算后得到的回归结果相同，所以信息安全管理能显著推动企业数字化转型，由此证实了论文提出假设 1。

表 3 基准回归分析结果

变量	Digital			
	(1)	(2)	(3)	(4)
L.ISO27001	2.1298*** (7.51)	2.2564*** (7.79)	2.2661*** (7.81)	2.1130*** (7.52)
Controls	控制	控制	控制	控制
Year	控制	—	—	控制
Ind	—	控制	—	控制
Pro	—	—	控制	控制
Firm	控制	控制	控制	控制
常数项	-4.4445*** (-8.20)	2.5504*** (16.80)	2.4903*** (20.05)	-4.0307*** (-8.28)
R2	0.2153	0.1816	0.1738	0.2115
Ods	31385	31169	31385	31169

注：*、**、*** 代表 10%、5%、1% 水平上显著，括号数值是 t 统计量，下同。

3.3 稳健性检验

考虑到传统的熵值法可能会影响赋权合理性，所以此次进行稳健性检验采取“企业数字化转型词频加总”这一方法设置指标，用 Sum_Digital 表示，整理回归结果见表 4 中的列 (1)，计算 L.ISO27001 回归结果，确定其在 1% 水平

显著为正。

结合国内外现有信息安全认证标准，从 [0, 1] 之间设置虚拟变量，依次有：企业内部 ciso (CISP)、国际 ciso 专家 (CIS-SP)、企业通过安全水平鉴定 (Security+)。以上变量替换构建模型中的 L.ISO27001。出于对数据一致性的考虑，选定 CISP、CISSP、Securi-ty+ 三个变量，并且采集前置一期数据，计算得到回归结果，见表 4 中的列 (2)~(4)。分析后发现，选定的三个变量均在 1% 水平显著为正，即基本回归结果具有稳健性。

表 4 稳健性检验结果

变量	Digital			
	(1)	(2)	(3)	(4)
L.ISO27001	29.5669*** (7.48)	—	—	—
L.CISP	—	2.7058*** (2.94)	—	—
L.CISSP	—	—	5.2015*** (3.02)	—
L.Security+	—	—	—	0.4095*** (10.45)
Controls	控制	控制	控制	控制
Year/Ind/Pro/ Firm	控制	控制	控制	控制
常数项	-55.5780*** (-8.35)	-4.1823*** (-8.40)	-4.2230*** (-8.43)	-4.3085*** (-8.46)
R2	0.2115	0.1836	0.1869	0.1880
Ods	31190	31190	31190	31190

4 同步推进路径

此次分析构建作用机制为“信息安全管理→声誉、人力资源→企业数字化转型”，构建同步推进路径，以构建的模型 (1) 和递归方程为基础，设定模型 (2) (3) (4)：

$$Digital_{it} = \lambda_0 + \lambda_1 ISO270001_{i,t-1} + \sum_{m=2} \lambda_m Control_{it} + \varepsilon_{it} \quad (2)$$

$$Med_{it} = \mu_0 + \mu_1 ISO270001_{i,t-1} + \sum_{m=2} \mu_m Control_{it} + \varepsilon_{it} \quad (3)$$

$$Digital_{i,t+1} = \gamma_0 + \gamma_1 Med_{it} + \gamma_2 ISO270001_{i,t-1} + \sum_{m=2} \gamma_m Control_{it} + \varepsilon_{it} \quad (4)$$

以上三个模型中，选择 2 组中介变量 (Med)，依次是声誉和技术 / 非技术人员在企业总人数中的占比，用 REP、Tech/Non_tech 表示。鉴于以上三个模型包含的变量传导途中面临时间延后的问题，所以“信息安全管理”在分析中做前置一期处理，而中介变量则依然采用当期数据结构，“企业数字化转型”滞后一期，控制变量同上文。

根据表 5 整理的企业声誉检验结果，列 (1) 显示 L.ISO27001 对 F.Digital 回归结果，确定其在 1% 水平显著为正，列 (2) 则是 L.ISO27001 对 REP 回归结果，为 1.4472，

同样在 1% 水平显著为正，代表信息安全管理可以增强声誉，有效规避网络安全风险导致的声誉受损。REP 对 F.Digital 回归结果数值是 0.0112，由此可知，如果信息安全管理相同，那么企业的声誉高，证明数字化转型水平高。由此，假设 2 得到验证。

表 5 信息安全管理、声誉和企业数字化转型机制检验结果

变量	F.Digital	REP	F.Digital
	(1)	(2)	(3)
L.ISO27001	1.7518*** (4.49)	1.4472*** (2.94)	1.6625*** (15.40)
REP	—	—	0.0112*** (5.60)
Controls	控制	控制	控制
Year/Ind/Pro/Firm	控制	控制	控制
常数项	-4.8512*** (-5.20)	-70.4482*** (-40.23)	-5.4853*** (-13.43)
R2	0.1785	0.2766	0.1762
Obs	13655	13655	13655

根据表 6 中整理的关于人力资源检验结果，其中列 (1) 为 L.ISO27001 对于 F.Digital 回归结果，数据在 1% 水平上显著为正。列 (2) 为 L.ISO27001 对于 Tech 回归结果，数值为 1.9079，列 (3) 即在控制 L.ISO27001 前置一期变量的情况下，Tech 对 F.Digital 的回归结果，数值为 1.8166，以上结果均在 1% 水平显著为正。综合分析可知，信息安全管理有利于增加企业中技术人员数量，从而推动企业数字化转型。所以，论文提出假设 3 得到验证。

表 6 信息安全管理、人力资源和企业数字化转型机制检验结果

变量	F.Digital	Tech	F.Digital
	(1)	(2)	(3)
L.ISO27001	1.8402*** (5.96)	1.9079*** (2.97)	1.8166*** (5.93)
Tech	—	—	0.0082*** (3.53)
Controls	控制	控制	控制
Year/Ind/Pro/Firm	控制	控制	控制
常数项	-4.9812*** (-8.55)	12.0879*** (3.03)	-5.0790*** (-8.56)
R2	0.1632	0.0424	0.1658
Obs	23520	23520	23520

5 结论与建议

5.1 结论

选择某上市公司在 2015—2024 年之间的数据进行分析，验证信息安全管理对于企业数字化转型的推动作用。经过研究分析，得到以下几点结论：①信息安全管理是企业内部非常重要的制度规范，能够规避企业在运营管理中可能面临的

网络风险，达到推动数字化转型的目的。②对于企业声誉的推动，是利用信息安全管理工具服务所有客户，如果企业声誉好，管理者不仅能制定更适合企业的决策，还能提高综合管理实力，这也是加快企业数字化转型的有效手段。③对于企业人力资源，深入实施信息安全管理，能实现企业管理模式的转型，即转变为技术、管理组合的新模式，改变生产关系。这样一来，企业对技术人才的需求量增加，人力资源需求也能逐渐向技术劳动力的方向转变，从而深入推进数字化转型。

5.2 建议

5.2.1 构建网络安全网络

企业数字化转型的实践中，组织的经营管理活动与互联网息息相关，这就需要构建安全性强的网络防范体系，例如防火墙、扫描系统漏洞等，保证企业信息安全，增强网络安全边界的防范水平。企业在实施数字化转型之后，网络安全界限的清晰性下降，建议大力应用虚拟专用网络或者列出访问控制表的方法，设置清晰性更强的网络安全边界，以免企业网络有未经授权的访问行为，或者受到黑客恶意攻击。

以往企业在构建网络安全模型方面，多是采用信任内部网络的方式，但是企业开始数字化转型后，可能面临的信息安全威胁增多，需要构建带有周期性的验证系统，并以透明加密技术作为辅助，对所有关键数据进行加密处理。数据的使用者不需要人为操作，便能保证所有文件数据安全。信息安全管理人员定期评估加密系统，确保加密处理的文件依然能保证私密性和安全性。另外，企业制定局部白名单，采集使用软件的版本信息、提供厂商信息等，列出软件清单。遵循白名单的基本管理要求构建数据库，软件通过审核后便可进入白名单库，再由管理人员对其进行定期安全评估，使白名单中的所有信息能保证安全性。

企业数字化转型越发深入，网络安全监控、日志管理等尤为重要，网络安全管理人员利用加密技术、流程管理系统，集中分析网络日志，排除日志中的安全隐患，如果发现风险，可以及时采取措施解决，保证数据安全。例如设置强密码，或者开启多因素身份验证，设置的密码需要定期更换，保证密码的复杂性，为企业中的关键数据提供多重保护。

5.2.2 建设信息等级化管理制度

信息化时代下企业的管理经营势必会形成大量数据，对大数据、云计算、人工智能等先进技术应用需求库也相应增加，从而提高了管理效率，但也会面临关键数据泄露的风险，其中人工智能技术还有可能出现滥用预测性维护的问题，给企业增加信息安全问题^[9]。有鉴于此，企业数字化转型期间需要不断完善信息管理制度，运用等级化理念，根据不同管理人员的工作内容与责任范畴，分别设置管理权限，保证数据安全。信息安全管理人员对管理权限进行分级，工作人员未获得权限的情况下，不支持系统中所有保密信息的操作，例如数据的编辑、下载等。尤其是企业中的关键保密

数据, 管理人员需要设置最高等级的保密权限^[10]。

企业开展数字化转型期间, 数据是非常重要的支持, 多元化信息技术能优化数据管理机制, 只是涉及到的条件比较多, 例如划分数据类别、设置管理权限以及多因素身份验证。对于企业而言, 也应结合实际优化数据管理程序, 保证数据完整性、安全性和可用性。为了实现这一目标, 建议在企业内部加密系统中增加数据备份功能, 并由专门的人员负责定期审核、监督, 排查信息安全风险, 所有数据可以定期备份, 以免信息泄露造成严重损失。

5.2.3 定期升级维护信息安全管理系统

企业在数字化转型中开展信息安全管理, 必须重视的一点适应动态变化, 管理人员定期升级、维护信息安全管理系统, 特别是系统模块、功能, 根据企业运行实际整合模块, 具体有信息安全系统、财务管理系统、人力资源系统等。上述系统之间协同运行, 能为企业管理、运营提供数据, 并制定科学合理的决策。另外, 企业数字化转型的实践中, 需要结合可能面临的风险, 完善风险入侵系统, 增强企业风险防范水平。根据系统运行的基本要求针对性的部署防火墙, 并采用外部链接检测管理和过滤脚本等技术, 防范风险程度高的信息。

参考文献:

[1] 连洁. 新时代企业电子档案管理与信息安全策略研究[J]. 办公自

动化, 2025, 30(7): 88-90.

- [2] 陈思睿. 科技信息管理对创新驱动发展的重要性探析[J]. 行政事业资产与财务, 2025(4): 137-139.
- [3] 许正利. 电力系统信息安全管理建设技术分析[J]. 电工技术, 2024(S2): 478-480.
- [4] 林建, 陈志永. 发展新质生产力助力企业品牌化——以中小企业信息安全和管理制度为例[J]. 中国品牌与防伪, 2024(12): 34-36.
- [5] 彭浩鸣, 王安蒙. 数智化转型企业网络信息安全管理建设策略[J]. 智慧中国, 2024(10): 71-72.
- [6] 程晓盼. 信息安全视域下企业人力资源档案数字化管理的优化策略探讨[J]. 企业改革与管理, 2024(16): 60-62.
- [7] 赵越, 马玉伟, 韩磊. 集团企业一体化信息系统安全管理策略研究[J]. 军民两用技术与产品, 2024(4): 66-69.
- [8] 彭青梅. 基于区块链技术的网络信息安全管理系统设计[J]. 信息记录材料, 2024, 25(4): 110-112.
- [9] 刘博舒. 计算机安全技术在企业信息管理中的应用[J]. 现代工业经济和信息化, 2022, 12(11): 93-95.
- [10] 曾莎莉. 新常态下数智化转型企业网络信息安全体系建设策略[J]. 信息系统工程, 2022(9): 111-114.

作者简介: 许珊珊(1983-), 女, 中国湖北长阳人, 本科, 工程师, 从事信息网络安全研究。