E-Commerce Letters 电子商务评论, 2024, 13(4), 6374-6384
Published Online November 2024 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2024.1341877

Hans汉斯

企业信息安全策略遵从性的影响因素研究

贺会阳

上海工程技术大学管理学院，上海

收稿日期：2024年9月6日；录用日期：2024年9月25日；发布日期：2024年11月29日

摘　要

随着社会经济与信息技术的发展，企业进行信息交流与沟通的途径逐渐多样化。但与此同时，企业的信息安全也面临着多重威胁。近些年来频繁发生在企业中的信息安全案例比比皆是，因此信息安全是企业当下必须重视的一个问题。而企业成员作为企业的主要组成部分，其是否遵从企业的信息安全策略对企业来说十分重要。本研究依据隐私计算理论构建研究模型，深入探究了信息安全策略遵从性的影响因素，并进行了相关的实证分析。本研究主要采用文献研究法、问卷调查法、统计分析法三种方法。根据相关文献研究，确定研究变量与研究模型，最终回收到有效问卷440份。本研究根据SPSS对回收的数据进行统计分析发现：遵从的感知成本、遵从的感知收益、不遵从的感知成本和隐私关注对企业成员的态度造成了显著影响，企业成员的态度对策略遵从性有显著影响。其中企业成员的态度作为中介变量，对遵从的感知收益起到部分中介作用，对遵从的感知成本、不遵从的感知成本和隐私关注起到完全中介作用。通过对研究结果的探讨，本文总结了研究结论并对企业的信息安全管理人员提出了合理建议。

关键词

企业信息安全，遵从性，隐私计算理论，感知收益，感知成本

Research on Influencing Factors of Enterprise Information Security Strategy Compliance

Huiyang He

School of Management, Shanghai University of Engineering Science, Shanghai

Received: Sep. 6th, 2024; accepted: Sep. 25th, 2024; published: Nov. 29th, 2024

Abstract

With the development of social economy and information technology, the ways for enterprises to communicate and exchange information are gradually diversifying. But at the same time, the enterprise's

文章引用: 贺会阳. 企业信息安全策略遵从性的影响因素研究[J]. 电子商务评论, 2024, 13(4): 6374-6384.
DOI: 10.12677/ecl.2024.1341877

information security is also facing multiple threats. In recent years, information security cases frequently occur in enterprises everywhere, so information security is an issue that enterprises must pay attention to at present. As the main part of the enterprise, it is very important for the enterprise whether its members comply with the enterprise's information security strategy. This study constructs a research model based on privacy computing theory, deeply explores the influencing factors of information security strategy compliance, and makes relevant empirical analysis. This study mainly adopts three methods: literature research, questionnaire survey and statistical analysis. According to the relevant literature research, the research variables and research models were determined, and 440 valid questionnaires were finally recovered. Based on the statistical analysis of the recovered data by SPSS, this study found that the perceived cost of compliance, the perceived benefit of compliance, the perceived cost of non-compliance and privacy concerns have a significant impact on the attitude of enterprise members, and the attitude of enterprise members has a significant impact on strategy compliance. Among them, the attitude of enterprise members, as an intermediary variable, plays a partial intermediary role in the perceived benefits of compliance, and a complete intermediary role in the perceived costs of compliance, non-compliance and privacy concerns. Through the discussion of the research results, this study summarizes the research conclusions and puts forward reasonable suggestions to the enterprise's information security managers.

Keywords

Enterprise Information Security, Compliance, Privacy Computing Theory, Perceived Benefits, Perceived Costs

1. 引言

1.1. 研究背景

信息技术的不断进步，极大地促进了企业信息交流的速度与效率。但是，科技的进步也给企业信息安全方面带来了极大的威胁与隐患。同时，信息对于企业的重要程度也显著提升，信息安全的问题也同样因此而日益突出。目前，企业面对的信息安全问题正在变得越来越复杂，企业对信息的严重依赖性要求他们必须重视与信息安全相关的问题。信息安全的问题不仅仅是关乎企业生存的问题，更是关乎企业成员未来发展的问题。

现如今，与信息安全相关的风险已成为威胁许多企业的重大问题，许多企业面临着信息安全方面的重大挑战，这些风险可能造成非常严重的后果，比如财产损失、信誉损失和金钱损失等。确保信息安全已成为许多企业的当务之急和最高管理优先事项之一。近些年来，发生在企业中众多的信息安全事件说明许多企业的信息安全工作开展的不平衡不充分，黑客攻击、病毒入侵、个人隐私泄露、数据泄密等问题在企业中层出不绝，信息事故对企业的正常运营产生了极大阻碍，让企业面临多重风险。

1.2. 研究目的及意义

1、研究目的

本研究针对信息安全问题，从企业成员对企业信息安全策略遵从性方面进行探究。鉴于大部分企业员工的信息安全意识比较薄弱，对企业的信息安全策略认识不够充分，不能很好地遵守企业所制定的信息安全方面的政策，企业成员作为企业在信息安全政策方面的薄弱环节需要引起企业管理层的高度重视

[1]。本研究的目的就是从企业成员的角度出发，找出影响企业成员策略遵从性的因素，并根据研究结果对企业的信息安全管理提出合理的建议与启发。

2、研究意义

当前国内对信息安全方面进的研究主要注意力还是集中在技术的手段和相关法律法规的研究，对于企业成员信息安全行为的实证分析较少[2]。本研究基于隐私计算理论，以调查问卷的形式收集实证样本，综合分析了影响企业成员对企业内的信息安全政策的遵从性的问题。因此，本研究对于信息安全领域有一定的理论意义以及现实意义。

本研究具有一定的理论意义。本文以隐私计算理论为基础，根据隐私计算理论构建研究模型，从更为全面与周到的角度分析了企业成员的信息安全策略遵循性的问题。并且通过实证分析，根据所收集到的结果，证明了所构建模型的合理性。

本研究具有一定的现实意义。本文针对当前社会存在的信息安全问题，综合分析了组织成员对企业的信息安全策略遵循性的影响因素，对企业的信息安全管理者如何引导企业成员遵守企业的信息安全策略具有一定的指导作用。深入探究了哪些因素会影响企业成员的信息安全策略遵从性，从而使企业的信息安全管理更加完善与高效。

2. 模型与假设

2.1. 研究变量

1、自变量

本研究选取遵从的感知收益、遵从的感知成本、不遵从的感知成本以及隐私关注为自变量。遵从的感知收益是指企业成员在遵循企业的信息安全策略时所感知的收益或好处，企业成员在遵循信息安全策略后可以得到一定的回报[3]。遵从的感知成本是指企业成员在遵循企业的信息安全策略时所感知的成本，不遵从的感知成本是指企业成员在不遵循企业的信息安全政策时所要付出的代价，隐私关注是一种与隐私泄露相关的一系列特殊的信息意识和感知，是个人针对隐私环境的主观感受。

2、中介变量

本研究选取态度作为中介变量。企业成员的态度是其遵循企业信息安全策略的关键，态度就是企业成员对于遵循信息安全策略的积极程度[4]。态度是个体对于特定事物的稳定心理倾向，这种心理倾向蕴含着个体的主观评价以及由此产生的行为倾向性。根据相关研究表明，企业成员的态度对其策略遵从性具有显著影响。

3、因变量

本研究以策略遵从性为因变量。策略遵从性是指企业成员遵从策略的程度，策略遵从性是保证企业信息安全的大前提[5]，在信息安全方面缺乏遵从性就相当于在管理方面没有执行力。

2.2. 企业信息安全策略遵从性理论模型

为了深入探究策略遵从性的影响因素，本研究基于隐私计算理论，本研究以遵从的感知收益、遵从的感知成本、不遵从的感知成本和隐私关注为自变量，态度为中介变量，策略遵从性为因变量，构建了基于隐私计算理论的信息安全策略遵从性的研究模型，如图 1 所示。

2.3. 企业信息安全策略遵从性研究假设

1、遵从的感知收益与态度

遵从的感知收益会影响企业成员对遵循企业信息安全策略的态度。比如有的企业成员会考虑遵从企

业的信息安全策略可能会给自己带来更大的竞争优势，因为遵循之后可以保证自己的信息安全得到更大的保证[6]，企业成员遵守企业的信息安全政策给企业成员带来诸多益处。研究发现遵从的感知收益越大，企业成员的态度就会越积极[7]。因此，提出以下假设：

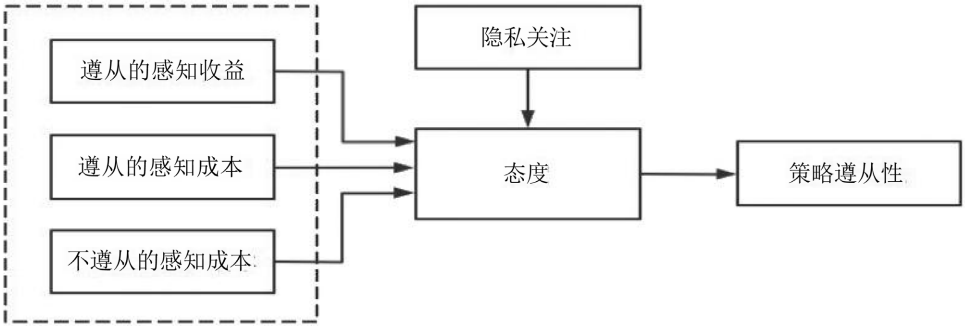

Figure 1. Research model on factors influencing compliance of enterprise information security strategies
图 1. 企业信息安全策略遵从性影响因素研究模型

假设 1：企业成员的态度与遵从的感知收益正相关

2、遵从的感知成本与态度

遵从的感知成本同样会对企业成员遵循企业的信息安全策略的态度造成影响。企业成员在遵循企业所制定的信息安全策略时会有一定的潜在损失。潜在损失是指个人的相关信息被泄露或者窃用[8]。企业成员在遵循企业的信息安全策略时常常会考虑以下几个问题：遵循企业的信息安全策略对自己是否很浪费时间、遵循企业的信息安全政策对自己是否是有负担的、遵循企业的信息安全策略对自己来说成本是不是很高。研究发现遵从的感知成本越小，企业成员的态度越积极。遵从的感知成本越大，企业成员的态度就会越消极[9]。因此，提出以下假设：

假设 2：企业成员的态度与遵从的感知成本负相关

3、不遵从的感知成本与态度

企业成员如果不遵循企业制定的信息安全策略自己会付出相应的成本。对于企业成员来说如果不遵守企业所制定的信息安全策略将会使企业成员在竞争中处于劣势，此外，如果不遵守企业的信息安全政策将会是自己的信息安全受到威胁[10]，还可能会使企业或个人受到财产或其他方面的损失。不遵从的感知成本越大，企业成员的态度就会越积极，不遵从的感知成本越小，企业成员的态度就会越消极[11]。因此提出以下假设：

假设 3：企业成员的态度与不遵从的感知成本正相关

4、隐私关注与态度

隐私关注是指个人在相应的隐私情境中主观感受到的公平程度。组织成员对于隐私的关注程度也会影响企业成员对信息安全策略的态度[12]。比如有的人对于生活中潜在的信息安全威胁及其消极后果比较了解，而有的人则根本不了解。再比如，有的人对于隐私及其带来的风险很关注，这部分人非常注重个人隐私安全也比较具有防范意识，这部分人对于信息安全策略的态度无疑是积极的[13]。而有的人则并不注重隐私安全和防范隐私危险的意识，这部分人对于信息安全策略的态度无疑是消极的。企业成员对于隐私越关注，其态度越积极[14]。企业成员对隐私越不关注，其态度越消极。因此，我们提出以下假设：

假设 4：企业成员的态度与隐私关注正相关

5、态度与策略遵从性

企业成员的态度影响企业成员遵从信息安全策略的决定[15]。企业成员信息安全策略的态度是积极

还是消极的态度会直接影响企业成员的决定。有的人认为遵守企业的信息安全策略对自己来说是十分有用且必要的，这部分人对企业的信息安全策略持有积极态度，那么他们在遵循企业的信息安全策略时就会更加积极[16]。有的人则认为遵循企业的信息安全策略对自己来说无所谓，这一部分人就对企业的信息安全策略持有消极态度，这种消极态度会对其遵循的决定产生消极影响[17]。因为态度会影响决策过程中的说服力[18]，而且要特别认识到个人对信息安全策略形成有利或不利的态度，以便更具有说服力。所以企业成员的态度会影响企业成员的策略遵从性[19]。因此，我们提出以下假设：

假设 5：企业成员的策略遵从性与企业成员的态度正相关

3. 问卷设计与数据分析

3.1. 问卷设计

本文为了达成研究目标，通过问卷调查法收集样本数据并进行实证分析。本研究主要在年龄和劳动力市场进入与否方面上设定限制，具体调查样本对象为出生于(1995~2009 年)的企业在职人员。为了确保调查样本的良好的代表性，在全中国地域范围和尽可能多元的行业上收集样本和数据。

此外，本文通过问卷调查收集样本的遵从的感知收益、遵从的感知成本、不遵从的感知成本、隐私关注、态度和隐私遵从性等各变量相关信息，并且信息数据的收集主要以线上问卷调查的方式进行。其中各个变量以及变量的各个维度的测量均采用国内外较为成熟、收到普遍认同并且在相关研究中得到证实的量表，如表 1 所示。

Table 1. Initial measurement scale
表 1. 初始测量量表

变量	测项
遵从的感知收益	1. 遵守信息安全策略的要求对我是有益的
	2. 遵从信息安全策略的要求，会使我更具有竞争优势
	3. 遵从信息安全策略的要求，会使得我的个人隐私得到更好的保护
遵从的感知成本	1. 对我来说遵从信息安全策略的要求是很费时间的
	2. 对我来说遵从信息安全策略的要求是有负担的
	3. 对我来说遵从信息安全策略的要求成本很高
不遵从的感知成本	1. 如果我不遵守信息安全策略的要求，对我将是不利的
	2. 如果我不遵守信息安全策略的要求，会使我在竞争中处于劣势
	3. 如果我不遵守信息安全策略的要求，可能对我造成损失
隐私关注	1. 总的来说，我知道潜在的安全威胁及其消极后果
	2. 我完全知道潜在信息安全问题的成本
	3. 我知道大家对隐私以及隐私带来的风险很关注
态度	1. 对我来说，遵守信息安全策略的要求是很必要的
	2. 对我来说，遵守信息安全策略的要求是非常重要的
	3. 对我来说，遵守信息安全策略的要求是非常有用的
策略遵从性	1. 我打算以后遵守信息安全相关的策略要求
	2. 我打算以后根据信息安全策略的要求保护信息和技术资源
	3. 我以后使用信息和技术时，我打算履行信息安全策略中规定的责任

3.2. 数据收集描述性分析

1、样本数据收集

由于本研究主要调查对象为企业员工，在正式调研中，采用与预调研类似的方式，继续选取员工在公司总体员工中占有一定比例的企业，采取滚雪球抽样的形式，收集样本数据。通过在“问卷星”平台制作问卷内容，修改问卷题项，将制作好的正式问卷以二维码、网址链接等形式邀请企业员工填写，来了解员工在企业中的感受，并对收集到的数据加以分析验证。本研究主要通过两种渠道发放问卷：一是在企业实习期间，将问卷发放至公司的不同部门的员工，并邀请他们进行转发填写；二是通过已经毕业并在企业就业的朋友、同学，邀请他们填写问卷并帮助转发到朋友圈和工作群中。问卷调查范围较广，主要集中在华东以及华南地区，包括江西、广东、江苏、浙江以及上海等省市。本次正式调研收集到的问卷总数为 484 份，去除掉所有选项选择同一分值的问卷以及在有反向计分题目前后出现矛盾的问卷，最终得到有效问卷为 440 份，有效率为 91%。

2、描述性分析

最大值和最小值可用于检查数据中是否存在异常情况。平均值是用于描述数据的集中趋势指标。标准差是用来描述数据的离散趋势指标。当比较两组不同单位的数据(或值差异太大)时，变异系数用于比较离散度。描述性分析通过平均值来描述数据的总体情况[20]。从上表可以看出，当前数据中没有异常值，数据值在平均值的 3 个标准偏差范围内波动。因此，可以直接描述和分析平均值。可以得出结论，数据中没有异常值，平均值可以直接进行描述和分析。

本研究在得到 440 份有效问卷后，对调查者的特征进行了统计。从问卷回收的样本数据显示，具体有以下特征，如表 2 所示。

Table 2. Descriptive statistical data
表 2. 描述性统计资料

	N	最小值	最大值	平均数	标准偏差
性别	440	1	2	1.66	0.476
年龄	440	1	4	2.40	0.647
身份	440	−2	2	1.48	0.608
教育程度	440	−2	3	1.87	0.621
有效的 N (listwise)	440				

3.3. 信度分析

在信度分析中，α 信度系数(Cronbach 系数)是目前最常用的信度系数。如果任何测试或量表的可靠性系数大于 0.8，则该测试或量表的可靠性非常好；可靠性系数大于 0.7 是可以接受的；如果大于 0.6，则应在不损失其值的情况下修改量表；如果低于 0.6，则需要重新设计刻度。因此，对于标准化项的 Cronbach 系数，该系数的值范围在 0~1 之间。越接近 1，可靠性越高。一般来说，如果低于 0.5，有必要考虑重新调整调查表。信度分析如表 3 所示。

从下表可知，各个变量标准化后克隆巴赫系数均在 0.7 以上，这表明变量具有良好的内部一致性信度，也就是说变量具有一定的可靠性。表明了测验结果的一贯性、一致性、再现和稳定性，即测验结果反映了被测者的稳定的、一贯性的真实特征。

Table 3. Reliability analysis
表 3. 信度分析

	尺度平均数	尺度变异数	更正后项目总数相关	平方后相关	Cronbach's Alpha	标准化后
CPB1	8.00	3.804	0.720	0.572	0.838	
CPB2	8. 11	3.390	0.828	0.688	0.737	0.868
CPB3	8.01	3.618	0.698	0.524	0.860	
CPC1	5.36	5.762	0.839	0.723	0.861	
CPC2	5.30	5.526	0.853	0.740	0.849	0.912
CPC3	5.28	6.028	0.779	0.608	0.909	
NCPC1	7.84	3.289	0.654	0.441	0.675	
NCPC2	7.68	3.867	0.579	0.336	0.752	0.788
NCPC3	7.58	4.108	0.649	0.429	0.689	
PC1	7.95	2.753	0.583	0.340	0.593	
PC2	8.18	2.348	0.526	0.287	0.646	0.725
PC3	7.81	2.374	0.521	0.281	0.651	
A1	8.41	2.930	0.757	0.580	0.773	
A2	8.28	2.851	0.698	0.489	0.832	0.858
A3	8.26	3.097	0.738	0.556	0.793	
SC1	8.25	3.151	0.712	0.507	0.813	
SC2	8.27	2.965	0.746	0.556	0.782	0.856
SC3	8.25	3.112	0.728	0.532	0.799	

3.4. 效度分析

1、KMO 与 Bartlett 检定

第一个：KMO 系数(Kaiser-Meyer-Olkin Measure of Sampling Adequacy)，取值范围在 0~1 之间，越接近 1 说明问卷的结构效度越好。

第二个：巴特利球形检验(Bartlett's Test of Sphericity)的显著性 Sig，如果小于 0.05，可以认为问卷具有良好的结构效度。检定图表如表 4 所示。

Table 4. KMO and Bartlett test
表 4. KMO 与 Bartlett 检定

Kaiser-Meyer-Olkin 测量取样适当性		0.868
Bartlett 的球形检定	大约卡方	1288.396
	df	153
	显著性	0.000

从上表可知，KMO 系数值为 0.868，位于 0~1 之间并且接近于 1，表明问卷的结构效度很好。巴特利球形检验的显著性值为 0.000 小于 0.05，更加表明问卷具有良好的结构效度。

2、相关性分析

相关分析是比较两个变量之间关系的常用方法。相关系数在 1 到−1 之间。当相关系数大于 0 时，两个变量之间存在正相关。如果相关系数等于 0，则这两个变量相互独立。如果相关系数小于 0，则两个变量之间存在负相关；相关系数的绝对值越大，两个变量之间的相关性越强。相反，相关系数的绝对值越大，两个变量之间的相关性就越弱。

Table 5. Correlation test
表 5. 相关性检验

		CPB	CPC	NCPC	PC	A	SC
CPB	皮尔森(Pearson)相关	1	−0.230*	0.251*	0.634**	0.725**	0.744**
	显著性(双尾)		0.020	0.011	0.000	0.000	0.000
CPC	皮尔森(Pearson)相关	−0.230*	1	0.033	−0.124	−0.331**	−0.323**
	显著性(双尾)	0.020		0.742	0.211	0.001	0.001
NCPC	皮尔森(Pearson)相关	0.251*	0.033	1	0.530**	0.446**	0.366**
	显著性(双尾)	0.011	0.742		0.000	0.000	0.000
PC	皮尔森(Pearson)相关	0.634**	−0.124	0.530**	1	0.675**	0.629**
	显著性(双尾)	0.000	0.211	0.000		0.000	0.000
A	皮尔森(Pearson)相关	0.725**	−0.331**	0.446**	0.675**	1	0.820**
	显著性(双尾)	0.000	0.001	0.000	0.000		0.000
SC	皮尔森(Pearson)相关	0.744**	−0.323**	0.366**	0.629**	0.820**	1
	显著性(双尾)	0.000	0.001	0.000	0.000	0.000	

注：*p < 0.05；**p < 0.01；***P < 0.001。

从上表 5 中可以得出结论：遵从的感知收益与态度相关系数为 0.725**，所以遵从的感知收益与态度正相关；遵从的感知成本与态度的相关系数为−0.331**，所以遵从的感知收益与态度负相关；不遵从的感知成本与态度的相关系数为 0.446**，所以不遵从的感知成本与态度正相关；隐私关注与态度的相关系数为 0.675**，所以隐私关注与态度正相关；态度与策略遵从性的相关系数为 0.820**，所以态度与策略遵从性正相关。

3.5. 回归分析

1、态度的线性回归模型分析

以性别、年龄、身份作为控制变量。遵从的感知收益、遵从的感知成本、不遵从的感知成本以及隐私关注作为自变量，态度作为因变量，利用 SPSS 进行回归分析，得到表 6。

从下表中可以得出，遵从的感知收益、遵从的感知成本、不遵从的感知成本以及隐私关注的显著性都小于标准 0.05，所以得出结论遵从的感知收益、遵从的感知成本、不遵从的感知成本以及隐私关注与企业成员的态度显著相关。结合表 5 所得结论可以得出：假设 1、假设 2、假设 3、假设 4 成立。

2、中介效应分析

以性别、年龄、身份作为控制变量。遵从的感知收益、遵从的感知成本、不遵从的感知成本、隐私关注以及态度作为自变量，策略遵从性作为因变量，利用 SPSS 进行回归分析，得到表 7。

Table 6. Analysis of attitude linear regression model
表 6. 态度的线性回归模型分析

模型		标准化系数 Beta	T	显著性	共线性统计资料		调整后的 r 方	Durbin-Watson
					允差	VIF		
1	(常数)		2.102	0.038			0.645	1.862
	CPB	0.471	5.920	0.000	0.550	1.817		
	CPC	−0.201	−3.259	0.002	0.912	1.096		
	NCPC	0.211	2.968	0.004	0.690	1.449		
	PC	0.216	2.384	0.019	0.423	2.362		
	性别	−0.014	−0.204	0.839	0.738	1.354		
	年龄	−0.004	−0.047	0.962	0.624	1.604		
	身份	0.072	1.035	0.303	0.722	1.386		

Table 7. Regression of CPB, CPC, NCPC, PC, and A on strategy compliance
表 7. CPB、CPC、NCPC、PC、A 对策略遵从性的回归

模型		标准化系数 Beta	T	显著性	共线性统计资料		调整后的 r 方	Durbin-Watson
					允差	VIF		
1	(常数)		−0.481	0.632			0.732	2.282
	CPB	0.324	4.007	0.000	0.402	2.487		
	CPC	−0.079	−1.387	0.169	0.820	1.219		
	NCPC	0.024	0.367	0.715	0.632	1.583		
	PC	0.078	0.961	0.339	0.399	2.504		
	A	0.550	6.165	0.000	0.331	3.023		
	性别	0.144	2.409	0.018	0.738	1.355		
	年龄	0.109	1.676	0.097	0.624	1.604		
	身份	−0.119	−1.959	0.053	0.714	1.401		

由上表数据可知，态度的显著性小于 0.05，所以态度对策略遵从性有显著影响，故假设 5 成立。在分析中加入中介变量态度之后，遵从的感知收益、遵从的感知成本、不遵从的感知成本以及隐私关注对策略遵从型的显著性都发生了变化。遵从的感知收益对策略遵从性的标准化系数由 0.583 下降到 0.324 且显著性为 0.000 仍显著，所以态度对遵从的感知收益是部分中介。遵从的感知成本对策略遵从性的标准化系数由−0.189 上升到−0.079 且显著性为 0.169，所以态度对遵从的感知成本是完全中介。不遵从的感知成本对策略遵从性的标准化系数由 0.140 下降到 0.024 且显著性为 0.715，所以态度对遵从的感知成本是完全中介；隐私关注对策略遵从性的标准化系数由 0.197 下降到 0.078 且显著性为 0.339，所以态度对隐私关注是完全中介。

4. 结论与展望

4.1. 研究结论

根据数据分析的结果我们可以验证前文提出的假设：企业成员对企业的信息安全策略的态度与遵从

的感知收益正相关；企业成员对企业的信息安全策略的态度与遵从的感知成本负相关；企业成员对企业的信息安全策略的态度与不遵从的感知成本正相关；企业成员对企业的信息安全策略的态度与隐私关注正相关；企业成员的策略遵从性与企业成员的态度正相关。企业成员的感知受益于感知风险影响企业成员的态度，进而影响对信息安全策略的遵从性。

企业成员会对自己遵从或者不遵从的行为进行一个收益与风险的评估，自我评估的结果决定了自己的态度。企业成员的策略遵从性与其本身的态度息息相关，企业成员的态度作为一个关键因素直接影响了企业成员的信息安全策略遵从性。因此，在企业的日常管理中应注意引领企业成员积极的态度。

4.2. 启示与展望

企业的信息安全管理者应关注激励企业成员遵循企业信息安全策略的因素，要激励企业成员积极遵循企业的信息安全政策。要想增强企业成员信息安全的意识，首先要在企业中推行一项切实可行的信息安全政策，并增强该政策的推行力度。对于那些激励因素管理者应该给予合理的刺激与激励以保证信息安全政策的实施。其次，企业的信息安全管理者要把重心放到企业成员身上，不能仅仅依赖技术因素。要充分认识到企业成员是企业信息安全关键的一环，充分发挥企业成员的导向和带头作用。企业成员在努力降低与信息安全相关的风险方面，可以成为巨大的力量。因为把握好企业成员这一关是加强信息安全的关键，企业成员是否遵守企业的信息安全政策对企业来说至关重要。

参考文献

[1] 陈琳. 影响员工遵从信息安全政策的要素研究[D]: [硕士学位论文]. 辽宁: 大连理工大学, 2011: 11-38.

[2] 欧露, 何翼, 秦林瑜, 等. 基于隐私计算理论的短视频平台隐私悖论路径研究[J]. 智能社会研究, 2023(6): 45-62.

[3] 石硕. 隐私计算、自我决定与社会交换理论视角下社交媒体用户隐私披露意愿研究[J]. 新媒体研究, 2023(19): 29-36.

[4] 时颖惠, 薛翔. 政策工具视角下我国信息安全政策研究——基于 81 份政策文本的量化分析[J]. 现代情报, 2022, 42(1): 130-138.

[5] 张艳红. 社交网站用户自我信息表露行影响因素研究[D]: [硕士学位论文]. 北京: 北京邮电大学, 2013: 30-35.

[6] 徐贤贤. 基于用户感知的 A 银行手机银行业务服务质量提升研究[D]: [硕士学位论文]. 杭州: 浙江工商大学, 2021: 51-69.

[7] 强月新, 肖迪. 社交网络中的隐私悖论: 隐私关注、自我表露意愿对社交推文发送的影响研究[J]. 国际新闻界. 2019, 41(12): 6-26.

[8] 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.

[9] 汪丽. “一带一路”国家网络安全政策法律动态及趋势[J]. 信息安全与通信保密, 2019(7): 17-21.

[10] 闫履鑫. 企业威慑与员工信息安全政策遵从意愿——辱虐管理的调节效应[D]: [硕士学位论文]. 大连: 东北财经大学, 2019.

[11] 黄玥, 周丽霞, 蒲攀. 基于 AHP 方法的我国信息安全政策方案优化决策研究[J]. 现代情报, 2015, 35(3): 77-81.

[12] Höne, K. and Eloff, J.H.P. (2002) Information Security Policy—What Do International Information Security Standards Say? *Computers & Security*, **21**, 402-409. https://doi.org/10.1016/s0167-4048(02)00504-7

[13] Sohrabi Safa, N., Von Solms, R. and Furnell, S. (2016) Information Security Policy Compliance Model in Organizations. *Computers & Security*, **56**, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

[14] Kenneth, J.K. and Thomas, E.M. (2015) Information Security Policy: An Organizational-Level Process Model. *Computers & Security*, **7**, 793-508.

[15] Johnston, A.C., Warkentin, M., McBride, M. and Carter, L. (2016) Dispositional and Situational Factors: Influences on Information Security Policy Violations. *European Journal of Information Systems*, **25**, 231-251. https://doi.org/10.1057/ejis.2015.15

[16] Kadam, A.W. (2007) Information Security Policy Development and Implementation. *Information Systems Security*, **16**, 246-256. https://doi.org/10.1080/10658980701744861

[17] Williams, P. (2001) Information Security Governance. *Information Security Technical Report*, **6**, 60-70. https://doi.org/10.1016/s1363-4127(01)00309-0

[18] Cram, W.A., Proudfoot, J.G. and D'Arcy, J. (2017) Organizational Information Security Policies: A Review and Research Framework. *European Journal of Information Systems*, **26**, 605-641. https://doi.org/10.1057/s41303-017-0059-9

[19] Mikko, S. and Pahnila, S. (2002) Compliance with Information Security Policies: An Empirical Investigation. *Computers*, **2**, 64-71.

[20] Da Veiga, A. and Eloff, J.H.P. (2010) A Framework and Assessment Instrument for Information Security Culture. *Computers & Security*, **29**, 196-207. https://doi.org/10.1016/j.cose.2009.09.002