第31卷第4期 管理科学 ISSN 1672-0334 Vol. 31 No. 4 91-102
2018年7月 Journal of Management Science July, 2018

# 信息安全压力与员工违规意愿：被调节的中介效应

甄 杰[1]，谢宗晓[2]，董坤祥[3]
1 重庆工商大学 商务策划学院，重庆 400067
2 中国金融认证中心 信息安全服务部，北京 100054
3 山东财经大学 管理科学与工程学院，济南 250014

**摘要**：信息技术和信息系统的应用对组织绩效的促进作用已经得到持续证明，信息已经成为重要资产。然而，组织员工有意或无意的信息安全违规行为往往会使企业承受巨大的信息安全风险，甚至给企业造成灾难性的损失。因此，员工的信息安全违规行为已经成为企业信息安全管理中需要重点关注的问题。已有研究探讨了员工信息安全违规行为的影响因素，但却存在研究结论不一致、脱离企业信息安全管理实践的局限，因而无法为企业如何控制和减少员工的信息安全违规行为提供有针对性的对策和建议。

基于应对理论和道德推脱理论，以道德推脱为中介变量、以信息安全意识为调节变量，构建被调节的中介效应模型，探讨信息安全压力对员工信息安全违规意愿的影响机制。以中国通过信息安全管理体系（ISO/IEC 27001）认证的企业员工为调研对象，收集318份有效问卷进行实证研究，综合运用逐步线性回归和被调节的路径分析方法进行统计分析和假设检验。

研究结果表明，信息安全压力对员工信息安全违规意愿有显著正向影响，并且道德推脱在两者之间起中介作用；信息安全意识对信息安全压力与道德推脱、道德推脱与信息安全违规意愿之间的关系均有负向调节作用；信息安全意识负向调节道德推脱在信息安全压力与信息安全违规意愿之间的中介作用，存在被调节的中介效应。也就是说，员工信息安全意识越高，道德推脱的中介作用越弱，反之越强。

研究结果明晰了信息安全压力对员工信息安全违规行为的影响机理，加深了对员工信息安全压力的理解，丰富了行为信息安全管理方面的研究，并对企业如何通过提高员工的信息安全意识、加强员工的职业道德培训来控制和减少员工的信息安全违规行为具有一定的指导意义。

**关键词**：信息安全压力；信息安全意识；违规意愿；道德推脱；应对理论
**中图分类号**：C931.6 **文献标识码**：A **doi**：10.3969/j.issn.1672-0334.2018.04.007
**文章编号**：1672-0334(2018)04-0091-12

**收稿日期**：2017-07-05 **修返日期**：2018-03-21
**基金项目**：国家自然科学基金（71672123）；重庆市基础科学与前沿技术研究项目（cstc2017jcyjAX0441）；重庆市社会科学规划项目（2017QNGL55）；重庆市教委人文社会科学研究项目（17SKG097）；重庆工商大学校内科研项目（1751030）

**作者简介**：甄杰，管理学博士，重庆工商大学商务策划学院讲师，研究方向为行为信息安全和电子商务等，代表性学术成果为“个性化产品在线定制意愿影响因素研究——基于计划行为理论的分析”，发表在2016年第6期《预测》，E-mail：zhenjie886@163.com
谢宗晓，管理学博士，中国金融认证中心信息安全服务部总经理，研究方向为网络与信息安全管理等，代表性学术成果为“制度压力、信息安全合法化与组织绩效——基于中国企业的实证研究”，发表在2016年第2期《管理世界》，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讲师，研究方向为信息安全风险管理和众包等，代表性学术成果为“众包竞赛中解答者创新绩效影响因素研究——感知风险的调节效应”，发表在2016年第2期《科学学与科学技术管理》，E-mail：dkxgood@163.com

## 引言

随着计算机网络和信息技术的快速发展,企业的正常运转和市场竞争力的提升愈发依赖于信息技术和信息系统的支持,信息已然成为企业的关键资产和重要资源。然而,频发的信息安全事件却时常将企业置于各种风险和威胁之中,信息安全也日渐成为企业高度关注的管理问题[1]。企业的信息安全风险由外部威胁(如黑客入侵、网络间谍活动)和内部威胁构成。其中,70%~80%的信息安全风险是由员工有意或无意的违规行为引发的[2]。因此,员工的信息安全违规行为已经超越外部威胁成为企业信息安全管理中需要重点解决的问题[3]。

事实上,员工的信息安全违规行为往往会对企业的信息安全管理造成巨大威胁[4],这是因为再先进的信息技术和管理信息系统,如果没有规范操作作为基本保障,其安全性也会大大折扣[5]。也就是说,即使企业采纳了先进的信息技术或部署了完备的管理信息系统,员工如果没有遵守信息安全管理制度(如重要数据备份、安全的操作规程等),也很容易引发严重的信息安全风险或事件。一般来说,制定科学合理的信息安全管理制度[6]并严格的执行是企业信息安全的重要保证[7],但是企业如果不能有效减少员工的信息安全违规行为,也就不能有效阻断频发的信息安全事件[8]。因此,探讨员工信息安全违规的关键影响因素和作用机制,对于企业预防和管理员工的信息安全违规行为具有重要的理论和现实意义。

## 1 相关研究评述

近年来,借鉴犯罪学、社会心理学、健康学和组织行为学等领域的相关理论探讨员工的信息安全行为是国内外行为信息安全研究的热点[9],涉及的主要研究问题包括:①企业如何确保员工遵守其内部的信息安全管理策略[10];②企业如何激发员工的信息安全保护行为;③企业如何设计相应的惩罚措施,以形成对员工信息安全违规行为的有效威慑[11];④员工产生信息安全违规行为的原因。尽管围绕上述问题的探讨取得一定研究成果,但是已有研究存在以下3个局限。

(1)研究结论不统一。IFINEDO[12]研究发现,感知威胁严重性对员工的信息安全遵守行为有正向影响。相反地,VANCE et al.[13]则证明,感知威胁严重性对员工的信息安全遵守行为有负向影响。这一研究结论的矛盾,在很大程度上是由于两项研究使用同一理论中的变量测量维度不一致造成的。由此可见,行为信息安全管理领域内的相关研究还存在较大的改进空间。

(2)精英偏见。已有研究主要基于信息安全专家和高层管理团队的思维模式,从而导致研究结论往往出现精英偏见[1]。换句话说,信息安全专家和高层管理人员代表了企业的高层管理,即使他们能够提供员工信息安全行为的有益见解,但是他们几乎接触或意识不到一般组织员工感知到的管理信息系统的脆弱性和信息安全管理带给他们的困惑[14]。因此,相关研究也就无法对员工的信息安全保护及信息安全违规行为做出全面、充分的解读和分析。

(3)系统分析员工信息安全违规影响因素和作用过程的研究比较匮乏[15]。已有研究较多探讨企业如何通过严厉的惩罚措施来威慑员工[16],进而减少信息安全违规行为的发生,但是较少涉及对员工信息安全违规(行为)意愿的影响机制的分析,如内在动机、影响因素和作用过程[17]。只有SIPONEN et al.[18]运用中和技术理论分析员工信息安全违规意愿的形成过程,即员工用否认责任、否认伤害等6种中和技巧来说服自己,以做出信息安全违规行为;D′ARCY et al.[7]从员工遵守信息安全管理策略会产生"额外"工作负荷的角度,解读员工的道德推脱对信息安全违规行为的影响。然而,上述研究有两个明显的局限性:①忽视了信息安全意识的作用。也就是说,上述两项研究没有结合企业信息安全管理的实践,没有探讨员工信息安全意识的影响和作用,因此也就没有办法解答为什么越来越多的国内外企业非常重视开展或推动员工的信息安全意识培训;②在行为信息安全的管理研究中,没有充分考虑"人"的正向能动可能性。换句话讲,员工态度和行为的转变(如执行一个"坏"的工作行为)需要经历态度和行为的转变过程,这个转变过程需要有合理和充分的理论分析和解读。只有这样,才能拓展行为信息安全相关理论的解释范畴。

信息安全违规行为包括不遵守信息安全管理制度的所有信息资源、技术、系统的不规范使用行为。基于上述分析,本研究对员工信息安全违规行为的影响机制展开分析,基于应对理论和道德推脱理论构建信息安全压力、道德推脱、信息安全意识和信息安全违规意愿之间的关系模型,采用问卷调查方法对研究模型进行验证,以期能够为企业有效减少和控制员工的信息安全违规行为提供有针对性的对策和建议。

## 2 理论基础和研究假设

本研究的理论基础是应对理论和道德推脱理论,应对理论主要用来分析员工道德推脱的前因,道德推脱理论主要用来解释员工如何说服自身的内在道德调控系统以允许信息安全违规行为的发生。

### 2.1 应对理论

应对理论详细描述了个体心理压力的认知和行为过程,因此该理论为员工信息安全压力的产生,即员工为遵守信息安全管理制度所产生的压力提供了一个合适的理论分析框架[7]。具体来说,应对理论主要分析个体面对压力时经历的应对过程和采取的应对策略,以及这些策略为何产生、有何作用[19]。该理论指出,应对过程首先要进行压力评估,主要包括首要评估和次要评估两个相关联的评估环节。在首要评估环节,个体会评价所面临事件的关联性,并

判断事件是否会带来压力;在次要评估环节,个体会判断对该压力事件的驾驭能力。经过上述两个评估环节,个体会形成对该事件的应对策略[20]。与此相对应,本研究关注的信息安全压力是员工经过首要评估和次要评估产生的结果,它是指为了满足企业信息安全管理要求,需要消耗员工认知资源和能力所引发的一种心理压力。与具有挑战属性的工作压力不同,信息安全压力往往由员工为了履行工作职责而使用信息技术或操作信息系统的工作负荷过载、复杂性和不确定性所造成[5]。因此,员工的信息安全压力更多的是一种具有阻断属性的工作压力。

在评估结果的具体应对策略上存在多种不同的反应分类,但是应用最多的应对策略分类是问题聚焦和情绪聚焦。问题聚焦的应对策略包括直接努力或改变所面临的压力环境。在特定的工作环境下,基于问题聚焦的努力消除障碍的同时,可以增加人们的工作知识和技能。情绪聚焦的应对策略包括改变思考或体验压力的方式,如转移注意力和逃离特定的压力情景[21]。也就是说,情绪聚焦的应对策略无法改变客观存在的压力环境[22],而问题聚焦的应对策略可以改变特定的压力环境[23]。基于上述分析,信息系统领域的学者已经采用该理论来分析相关问题[24]。已有研究已经识别了几种不同的应对策略,包括精神放松技巧、修改工作任务以及创造或适应技术。同时,还有研究表明,当评估结果威胁到个人发展或工作推进时,如果员工判断他们对于这些压力情景的控制非常有限,则他们倾向于采用情绪聚焦的应对策略[25]。

### 2.2 道德推脱理论

BANDURA[26]在社会认知理论的框架下提出了道德推脱的概念,用于解读个人的不道德行为。道德推脱是指个体会产生一种特定的认知倾向,包括重新定义自己的不道德行为以使其伤害显得更小[27],并最大限度地减少自己在某项不道德行为后果中的责任[28]。因此,道德推脱理论往往用于解释为什么人们在明知错误的情况下,仍然会做出某些错误行为[29]。该理论认为,当个人在道德上采取推脱时,他就切断了该行为与其有害后果间的关系[30]。

组织领域的相关研究已经证明,道德推脱为分析员工的消极工作、违规、不道德行为提供了一种全新视角[31]。当某种违规行为产生于组织时,员工往往会将违规行为造成的伤害进行去人性化的认知和解读,从而使人们摆脱了因违反自身道德标准而产生的内疚和自责情绪,心安理得地做出不道德行为[32]。基于上述分析,本研究采用道德推脱理论分析员工在做出信息安全违规行为时的自我认知调整和自我说服心理过程。

### 2.3 研究假设

#### 2.3.1 信息安全压力对违规意愿的直接效应

在企业的信息安全管理中,当员工严格按照信息安全管理制度执行日常工作任务时,有些员工会感知到信息安全压力,即遵守信息安全管理制度的工作任务负荷过重、管理要求复杂难懂、安全要求不够具体明确,该过程是应对理论的首先评估过程[5]。已有研究表明,员工往往会将负面情绪(如时间的浪费、精力的耗费和挫折)归因于为了满足岗位信息安全需求而付出的"额外"努力[7]。与此同时,员工也会感知到他们对于企业的信息安全管理制度的执行要求没有任何的控制权或话语权,该过程是应对理论的次要评估过程。也就是说,耗费员工时间和精力的信息安全操作步骤增加了员工的工作负担,为员工带来了信息安全压力,员工自觉执行信息安全管理制度的可能性就会下降[33]。尤其是在企业的信息安全管理制度比较复杂的情况下,员工只有两种选择:第一,花费大量的时间和精力充分地理解复杂的管理程序和繁琐的技术要求,这样做可能会在一定程度上降低日常工作的进度;第二,不遵守企业的信息安全管理制度,冒着一定风险采取信息安全违规行为,而不会对工作进度产生太大影响。因此,本研究提出假设。

$H_1$　信息安全压力对员工的信息安全违规意愿有正向影响。

#### 2.3.2 道德推脱的中介作用

信息安全压力会引发员工的信息安全违规行为[3],然而信息安全压力对违规(行为)意愿的具体作用机制还有待于更加深入的探讨。频发的员工信息安全违规行为显然违反了企业信息安全管理制度,背离了职业道德准则。员工对规章制度的畏惧心理和对违规惩罚的恐惧心理,以及内心道德准则的自我驱使都没有促使其遵守企业的信息安全管理制度[9]。这就说明,一方面,道德推脱使员工的信息安全违规行为与外部惩罚之间失去联系,此时的自我道德调控过程已经失效[34],员工可以摆脱违规行为造成的内疚和自责;另一方面,当员工的信息安全违规不是一个偶发事件时,即信息安全违规时常发生于企业和团队的内部,此时员工往往会进行责任分散,以推脱应当承担的责任[34]。

整体而言,信息安全压力的存在意味着员工遵守信息安全管理制度有一定难度,当员工没有办法理解其重要性时,信息安全管理制度对于企业生存和发展的重要性就会大打折扣[7]。一般来说,信息安全压力会对员工的正常工作表现产生影响[7]。例如,员工遵守企业信息安全管理制度花费的时间,导致其不能及时完成工作任务或通过加班来完成工作任务。然而,一旦面临工作任务重或工作周期短的情况,通过拖延或加班没有办法完成既定工作。此时,这种累积的信息安全压力将会触发员工的负面行为反应[5]。事实上,员工受到的工作规范约束、接受的岗前培训和职业培训,以及内心具备的职业道德又不允许员工轻易做出信息安全违规行为。此时,信息安全违规行为的发生需要员工完成道德推脱的过程。进一步,员工的道德推脱通过道德辩护、责备归因、责任转移和责任分散等相互关联的机制产生作用[31],这就助推了员工不同类型信息安全违

规行为的发生。综上,员工的信息安全压力通过道德推脱的过程机制最终影响信息安全违规意愿。因此,本研究提出假设。

$H_2$ 道德推脱在信息安全压力与员工信息安全违规意愿之间起中介作用,即信息安全压力通过道德推脱间接正向影响员工信息安全违规意愿。

2.3.3 信息安全意识对信息安全压力与道德推脱的调节作用

信息安全领域的研究表明,员工违规行为导致的信息安全事件已经成为企业信息安全管理的主要威胁[35],提高员工的信息安全意识尤为重要[36],这也是国内外众多企业开展信息安全意识培训的原因[37]。信息安全论坛(Information security forum,ISF)将信息安全意识定义为组织所有员工理解信息安全的重要性,清楚组织所适用的安全级别[38],知悉并履行个人在日常工作中的安全职责[39]。

如前所述,员工的信息安全压力水平越高,越能够促使其进行道德推脱。但信息安全压力的产生也存在缓解条件和抑制因素,即信息安全意识[40]。员工高水平的信息安全意识有助于抑制信息安全压力的产生,从而进一步阻碍道德推脱。DINEV et al.[41]证明员工的信息安全意识越高,越有利于企业信息资源的保护;PUHAKAINEN et al.[42]证明信息安全意识培训可以显著提高员工的信息安全意识,提高员工遵守信息安全管理制度的能力,这也在某种程度上减轻了员工的信息安全压力;谢宗晓等[43]验证了员工信息安全意识对信息安全管理制度有效性的积极影响。由此可见,员工的信息安全意识越强,越能够阻碍信息安全压力的产生,进而减少道德推脱过程的进行。因此,本研究提出假设。

$H_3$ 信息安全意识负向调节信息安全压力与道德推脱之间的关系,即员工的信息安全意识水平越高,信息安全压力对道德推脱的影响越弱。

2.3.4 信息安全意识对道德推脱与员工信息安全违规意愿的调节作用

道德推脱与员工信息安全违规意愿密切相关,然而不同员工在信息安全违规方面的表现却存在很大差异[7]。由前述分析可知,道德推脱能够切断员工信息安全违规行为与其内在道德标准的关联,使员工不会因为信息安全违规而感到自责和内疚[44]。在企业信息安全管理中,如果员工具有强烈的信息安全意识,这就意味着员工理解并熟知日常工作中的信息安全管理制度,并对自身的工作职责有着清楚的认知[45]。此时,员工的道德推脱过程将会受到信息安全意识的“干扰”,不能顺利完成,道德推脱与信息安全违规意愿之间的关系就会受到抑制。因此,本研究提出假设。

$H_4$ 信息安全意识负向调节道德推脱与信息安全违规意愿之间的关系,即员工的信息安全意识水平越高,道德推脱对信息安全违规意愿的影响越弱。

2.3.5 被调节的中介作用

在前述分析中,一方面,基于应对理论和道德推脱理论的分析发现,员工的信息安全压力通过道德推脱的中介机制影响信息安全违规意愿;另一方面,基于信息安全意识的相关研究可知,高水平的信息安全意识可以抑制信息安全压力与道德推脱、道德推脱与信息安全违规意愿之间的关系。综合这两方面的论述,信息安全意识可能会对信息安全压力-道德推脱-信息安全违规意愿的整个中介机制起调节作用,换句话讲,可能存在被调节的中介效应。

员工的高信息安全意识水平为信息安全压力的产生提供了某种抑制条件,员工由此有更小的可能性将信息安全压力转化为道德推脱的过程;而员工道德推脱水平的降低,也降低了员工的信息安全违规意愿。反之,员工的信息安全意识水平较低时,便会有较高的信息安全压力感知,这就增加了员工道德推脱的可能性,进而导致较高水平的员工信息安全违规意愿。例如,微软公司在帮助客户建立信息安全方案时指出,建立信息安全意识培训方案的主要目标是通过强化大家认可的、与公司业务有关的安全活动,即降低产生信息安全压力的可能,从而改变全体员工的行为[39]。企业信息安全控制的效果依赖于员工的信息安全意识[35],信息安全意识的提高有利于员工执行信息安全管理制度以及建立重视信息安全管理的组织文化[46]。上述研究都在一定程度上验证了信息安全压力与员工信息安全违规意愿之间存在被调节的中介效应。因此,本研究提出假设。

$H_5$ 信息安全意识负向调节信息安全压力通过道德推脱影响员工信息安全违规意愿的中介效应,即员工信息安全意识越强,信息安全压力通过道德推脱影响员工信息安全违规意愿的中介效应越弱。

综上所述,提出研究模型,见图1。与已有相关研究[5,7]相比,本研究模型有两点创新:①在企业信息安全管理情景下,基于应对理论的两个评估环节,明确了员工信息安全违规的主要影响因素是信息安全压力,进而构建信息安全压力-道德推脱-信息安全违规意愿这一影响路径;②识别了信息安全意识的调节效应。这就意味着,明确了信息安全管理情景下道德推脱理论和应对理论的限制条件和适用范围,这对于既定框架下深入理解员工的信息安全违规行为有重要作用。上述两点创新对于明确企业信息安全管理中员工的重要性,从而更好地从行为信息安全的视角解决企业信息安全管理中“人”的问题有重要意义。

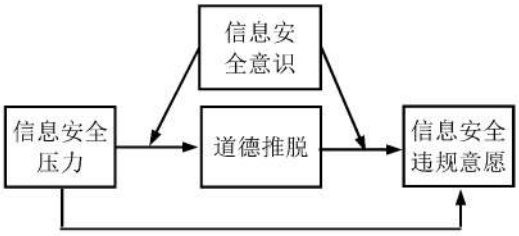


**图1 研究模型**

**Figure 1 Research Model**

## 3 研究方法

### 3.1 样本选取和数据收集

本研究采用问卷调查的方法进行数据收集,问卷调研对象是中国通过信息安全管理体系认证(GB/T 22080-2008/ISO/IEC 27001:2005)的企业的内部员工,说明被访者的工作单位正在实施信息安全管理制度,调研对象的工作环境符合本研究的情景要求。问卷调研过程依托专业的调研平台,采用在线填写问卷的形式,调研时间为2017年3月1日至2017年3月31日。问卷采用Likert 7点评分法,1为非常不同意,7为非常同意。

为了保证所填写问卷的有效性,对问卷的收集进行必要的控制。例如,每个IP地址只能对应一份有效问卷进入数据的分析过程;填写不完整的问卷不能提交等。在此基础上,对回收的356份问卷进行筛选,剔除恶意回答、前后不一致等的38份无效问卷后,最终得到有效问卷318份,问卷的有效回收率为89.326%。被访者的描述性统计结果见表1。

**表1 样本描述性统计结果**

**Table 1 Results for Descriptive Statistics of the Samples**

| 控制变量 | 分类指标 | 人数 | 比例/% |
|---|---|---|---|
| 性别 | 男 | 191 | 60.063 |
| | 女 | 127 | 39.937 |
| 年龄 | 23岁~30岁 | 136 | 42.767 |
| | 31岁~40岁 | 155 | 48.742 |
| | 41岁及以上 | 27 | 8.491 |
| 教育程度 | 专科及以下 | 13 | 4.088 |
| | 本科 | 187 | 58.805 |
| | 研究生 | 118 | 37.107 |
| 所属行业 | 软件相关 | 123 | 38.679 |
| | 金融相关 | 104 | 32.704 |
| | 通信相关 | 66 | 20.755 |
| | 电力相关 | 25 | 7.862 |
| 工作类型 | 市场营销相关 | 54 | 16.981 |
| | 技术研发相关 | 132 | 41.509 |
| | 客户管理相关 | 59 | 18.554 |
| | 系统管理相关 | 73 | 22.956 |

### 3.2 变量及其测量

为了保证测量工具的信度和效度,本研究尽量采用已有研究中被广泛使用和验证的研究量表,并结合企业信息安全管理这一特定情景进行调整。对信息安全压力的测量,根据D'ARCY et al.[7]和LEE et al.[5]的量表修改得到,包括3个题项,涉及工作负荷量、复杂性和不确定性3个维度;对道德推脱的测量,根据BANDURA[28]、MOORE et al.[32]和DETERT et al.[47]的量表改编,概括为3个题项,涉及道德辩护、责任转移和忽视结果3个维度;对信息安全意识的测量,根据SPEARS et al.[48]和D'ARCY et al.[49]的量表改编,包括3个题项;对员工信息安全违规意愿的测量题项来自于SIPONEN et al.[18]和CHENG et al.[6]的量表,采用密码管理、工作站注销和用移动设备拷贝数据3种情景模拟的方式,考察员工的违规意愿。

在控制变量方面,由于不同行业的信息化发展水平以及信息系统的采纳程度不同,进而造成不同行业中企业对于员工信息安全知识需求的不同。组织员工从事工作的类型会对其信息安全行为有影响,如市场营销和数据管理两种工作类型对于员工信息安全行为的要求完全不同。教育程度会对员工的认知和学习领悟能力有一定影响。一般来说,员工的年龄越大,工作经验也就越丰富,对于信息安全行为会有影响。基于上述分析,本研究将企业员工所属行业、工作类型、教育程度、年龄和性别作为控制变量。

本研究问卷量表的测量题项见表2。

## 4 实证结果和分析

### 4.1 共同方法偏差

基于问卷调查的实证研究中,如果观测变量由相同的被试者填答容易导致共同方法偏差问题。为了排除共同方法偏差的影响,本研究在统计控制环节采用Harman单因素检验的方法进行检验[50]。检验结果表明,第1个因子的方差解释度为38.933%,小于40%,说明研究数据不存在共同方法偏差问题,可以进行后续的数据分析工作。

### 4.2 信度和效度检验

本研究对量表的信度和效度进行检验,主要采用组合信度(*CR*)和项目载荷评价量表的信度;通过验证性因子分析,检验测量量表的结构效度,用潜变量平均变异萃取量(*AVE*)的平方根是否大于潜变量之间的相关值检验区分效度,用*AVE*评价量表的聚合效度。测量量表的不同指标见表2和表3。

由表2可知,信息安全压力、道德推脱、信息安全意识和信息安全违规意愿的组合信度分别为0.931、0.882、0.860和0.909,4个潜变量的Cronbach's $\alpha$值分别为0.889、0.802、0.758和0.849,均大于0.700的基准值。上述两个指标说明测量量表具有较好的信度。由表2可知,4个潜变量的*AVE*分别为0.818、0.714、0.672和0.769,均大于0.500的基准值;每个潜变量所包含测量题项的因子载荷均在0.700的基准值之上,表明量表具有较好的结构效度。对交叉载荷进行检验的结果见表3,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,表明本研究测量模型具有较高的聚合效度和区分效度。

**表2 量表的信度和效度**

**Table 2 Reliability and Validity of Scales**

| 变量名称 | 测量题项 | 因子载荷 | *AVE* | *CR* | Cronbach's α |
|---|---|---|---|---|---|
| 信息安全压力 | ①为了遵守企业信息安全管理制度,我增加了大量的工作 | 0.887 | 0.818 | 0.931 | 0.889 |
| | ②为了满足企业信息安全管理的要求,我感受到知识方面的压力 | 0.915 | | | |
| | ③企业信息安全管理制度的持续改进,造成了我工作的不确定性 | 0.910 | | | |
| 道德推脱 | ①企业信息安全管理制度太严格,有很多不合理的地方 | 0.883 | 0.714 | 0.882 | 0.802 |
| | ②偶尔违反信息安全管理制度,不会给企业带来损失和伤害 | 0.848 | | | |
| | ③不遵守信息安全管理制度在同事中很普遍,大家都这样做 | 0.802 | | | |
| 信息安全意识 | ①我认为企业信息安全管理的流程化是必要的 | 0.847 | 0.672 | 0.860 | 0.758 |
| | ②我认为企业信息安全管理的规范化是必要的 | 0.786 | | | |
| | ③我认为企业开展信息安全意识培训是必要的 | 0.806 | | | |
| 信息安全违规意愿 | ①我可能不会定期修改系统的登录密码 | 0.823 | 0.769 | 0.909 | 0.849 |
| | ②我可能会不注销工作站而直接关设备 | 0.890 | | | |
| | ③我可能会用移动设备来拷贝工作数据 | 0.916 | | | |

**表3 交叉载荷检验结果**

**Table 3 Test Results for Cross Loading**

| 测量题项 | 信息安全压力 | 道德推脱 | 信息安全意识 | 信息安全违规意愿 |
|---|---|---|---|---|
| 信息安全压力① | **0.887** | 0.676 | 0.672 | 0.534 |
| 信息安全压力② | **0.915** | 0.588 | 0.658 | 0.550 |
| 信息安全压力③ | **0.910** | 0.521 | 0.663 | 0.648 |
| 道德推脱① | 0.655 | **0.883** | 0.654 | 0.426 |
| 道德推脱② | 0.671 | **0.848** | 0.653 | 0.508 |
| 道德推脱③ | 0.678 | **0.802** | 0.695 | 0.530 |
| 信息安全意识① | 0.744 | 0.636 | **0.847** | 0.586 |
| 信息安全意识② | 0.790 | 0.572 | **0.786** | 0.595 |
| 信息安全意识③ | 0.783 | 0.529 | **0.806** | 0.691 |
| 信息安全违规意愿① | 0.612 | 0.552 | 0.671 | **0.823** |
| 信息安全违规意愿② | 0.615 | 0.379 | 0.680 | **0.890** |
| 信息安全违规意愿③ | 0.552 | 0.464 | 0.592 | **0.916** |

### 4.3 描述性统计

信息安全压力、道德推脱、信息安全意识和信息安全违规意愿4个潜变量的平均值、标准差和相关系数见表4。由表4可知,信息安全压力与道德推脱显著正相关,$r = 0.747, p < 0.010$;道德推脱与信息安全违规意愿显著正相关,$r = 0.542, p < 0.010$;信息安全压力与信息安全违规意愿显著正相关,$r = 0.645, p < 0.010$;道德推脱与信息安全意识显著负相关,$r = -0.722, p < 0.010$;信息安全意识与信息安全违规意愿显著负相关,$r = -0.712, p < 0.010$。这些相关性与理论预期的关系相一致,为验证研究假设提供了初步证据。

**表4　均值、标准差和相关系数**

**Table 4　Mean, Standard Deviation and Correlation Coefficients**

| | 均值 | 标准差 | 信息安全压力 | 道德推脱 | 信息安全意识 |
|---|---|---|---|---|---|
| 信息安全压力 | 4.239 | 1.204 | | | |
| 道德推脱 | 4.128 | 0.993 | 0.747** | | |
| 信息安全意识 | 4.191 | 1.322 | 0.625** | −0.722** | |
| 信息安全违规意愿 | 4.399 | 1.270 | 0.645** | 0.542** | −0.712** |

注:** 为 $p < 0.010$,下同。

**表5　回归分析结果**

**Table 5　Results of Regression Analysis**

| | 因变量:道德推脱 | | | 因变量:信息安全违规意愿 | | | |
|---|---|---|---|---|---|---|---|
| | 模型1 | 模型2 | 模型3 | 模型4 | 模型5 | 模型6 | 模型7 |
| 自变量 | | | | | | | |
| 信息安全压力 | | 0.589*** | 0.200** | | 0.518*** | 0.434*** | 0.302** |
| 道德推脱 | | | | | | 0.178** | 0.138* |
| 信息安全意识 | | | −0.143* | | | | −0.155* |
| 信息安全压力×信息安全意识 | | | −0.516*** | | | | −0.580** |
| 道德推脱×信息安全意识 | | | | | | | −0.422** |
| 控制变量 | | | | | | | |
| 性别 | −0.067 | −0.089 | −0.091 | −0.147 | −0.157 | −0.165 | −0.148 |
| 年龄 | −0.168 | −0.163 | −0.152 | 0.143 | 0.096 | 0.123 | 0.145 |
| 教育程度 | −0.013 | −0.032 | −0.016 | −0.004 | −0.007 | −0.013 | 0.004 |
| 工作类型 | 0.103 | 0.105 | 0.109 | 0.107 | 0.096 | 0.105 | 0.106 |
| 所属行业 | 0.179* | 0.094 | 0.106 | 0.094 | 0.082 | 0.075 | 0.093 |
| $R^2$ | 0.103 | 0.347 | 0.567 | 0.052 | 0.268 | 0.292 | 0.475 |
| $\Delta R^2$ | | 0.244 | 0.220 | | 0.216 | 0.024 | 0.183 |

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

### 4.4　研究假设检验

本研究进行逐步线性回归,考虑到需要进行调节效应检验,在进行回归分析之前对控制变量以外的所有变量进行中心化处理,具体回归分析结果见表5。表5中,模型1以道德推脱为因变量,以控制变量为自变量;模型2在模型1的基础上,增加信息安全压力为自变量,用来检验信息安全压力与道德推脱之间的关系;模型3在模型2的基础上,增加信息安全意识以及信息安全压力与信息安全意识的交互项为自变量,检验信息安全意识对信息安全压力与道德推脱之间关系的调节作用。模型4以信息安全违规意愿为因变量,以控制变量为自变量,模型5在模型4的基础上,增加信息安全压力为自变量,模型6在模型5的基础上增加道德推脱为自变量,模型4、模型5和模型6用来检验道德推脱的中介效应。模型7以信息安全违规意愿为因变量,自变量包括控制

变量、信息安全压力、道德推脱、信息安全意识以及信息安全压力与信息安全意识的交互项、道德推脱与信息安全意识的交互项,检验信息安全意识的调节作用。同时,模型3和模型7也是检验被调节的中介效应的重要步骤。

(1)检验$H_1$。模型5的回归结果表明,信息安全压力与信息安全违规意愿显著正相关,$\beta = 0.518$,$p < 0.001$,$\Delta R^2 = 0.216$,大于0,表示模型的解释力增强。因此,$H_1$得到验证。

(2)检验$H_2$。信息安全压力与信息安全违规意愿显著正相关,模型2的回归结果表明,信息安全压力与道德推脱显著正相关,$\beta = 0.589$,$p < 0.001$。以信息安全违规意愿为因变量、以信息安全压力和道德推脱为自变量进行回归分析,模型6的回归结果表明,信息安全压力与信息安全违规意愿显著正相关,$\beta = 0.434$,$p < 0.001$;道德推脱与信息安全违规意愿显著正相关,$\beta = 0.178$,$p < 0.050$。对比模型5与模型6的回归结果可知,信息安全压力回归系数由0.518降至0.434,说明信息安全压力对信息安全违规意愿的影响通过道德推脱的部分中介机制产生作用,$H_2$得到验证。

(3)检验$H_3$和$H_4$。模型3的回归结果表明,信息安全压力与信息安全意识的交互项系数为$-0.516$,$p < 0.001$,说明信息安全意识对信息安全压力与道德推脱之间关系有负向调节作用,$H_3$得到验证;模型7的回归结果表明,道德推脱与信息安全意识的交互项系数为$-0.422$,$p < 0.010$,说明信息安全意识对道德推脱与信息安全违规意愿之间关系有负向调节作用,$H_4$得到验证。为了更加准确判断调节效应的显著性,以平均数加减标准差为标准,将信息安全意识划分为高、低两个水平,然后进行简单斜率分析,结果见图2。由图2可知,在高信息安全意识水平下,信息安全压力与道德推脱以及道德推脱与信息安全违规意愿的关联性均较强,简单斜率分别为0.764($p < 0.010$)和0.568($p < 0.010$);在低信息安全意识水平下,信息安全压力与道德推脱以及道德推脱与信息安全违规意愿的关联性较弱,简单斜率分别为0.143($p > 0.050$)和0.087($p > 0.050$)。因此,$H_3$和$H_4$进一步得到验证。

(4)检验$H_5$。本研究采用EDWARDS et al.[51]提出的被调节的路径分析方法检验$H_5$(即被调节的中介效应),采用Spss的Process插件Bootstrap程序进行检验[52],设定Bootstrap的次数为5 000次,置信区间为95%[53],运算出不同信息安全意识水平下路径系数、标准误差和中介效应的置区间,结果见表6。

由表6可知,在低信息安全意识水平下,间接效应在95%水平上的置信区间包含0,即信息安全压力通过道德推脱影响信息安全违规意愿的作用不显著,$\beta = -0.071$,$p > 0.050$;在高信息安全意识水平下,间接效应在95%水平上的置信区间不包含0,系数为$-0.237$,$p < 0.010$,即信息安全压力通过道德推脱影响信息安全违规意愿的作用显著。也就是说,随着信息安全意识水平的提升,道德推脱的中介作用逐渐显著,$H_5$得到验证。

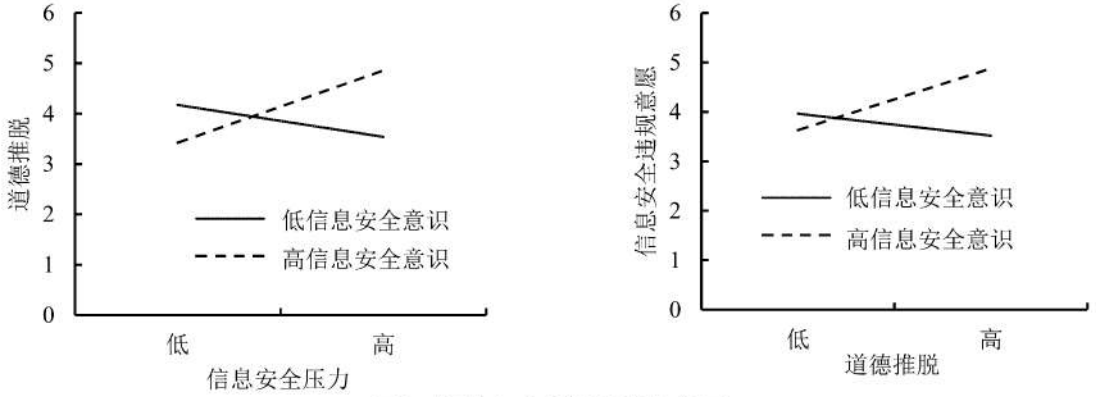


**图2 信息安全意识的调节作用**

**Figure 2 Moderating Effect of Information Security Awareness**

**表6 被调节的中介效应检验结果**

**Table 6 Test Results for Moderating Mediation Effects**

| 效应 | 信息安全意识 | 效应系数 | 标准误差 | 95%置信区间 | |
|---|---|---|---|---|---|
| | | | | 下限 | 上限 |
| 间接效应 | 低 | −0.071 | 0.072 | −0.050 | 0.132 |
| | 高 | −0.237** | 0.080 | 0.087 | 0.313 |
| | 差异 | 0.142 | 0.010 | 0.094 | 0.125 |

## 5 结论

本研究以应对理论和道德推脱理论为基础,以中国通过信息安全管理体系认证企业(ISO/IEC 27001)的员工为对象,采用问卷调查方法,对信息安全压力与员工信息安全违规意愿之间的作用机制进行研究,研究结果如下。

(1)信息安全压力对员工信息安全违规意愿有显著正向影响,并且道德推脱在信息安全压力与信息安全违规意愿之间起中介作用。员工信息安全压力越大,其信息安全违规的意愿越强烈。这与D'ARCY et al.[7]和LEE et al.[5]在组织管理情景下得出的信息安全压力与反生产行为/不道德组织行为关系的研究结论一致。企业内部诸多信息安全的要求造成了员工遵守信息安全管理制度的压力,这会加大员工信息安全违规的可能性。在此过程中,道德推脱过程切断了违规行为与负面后果(如愧疚和自责)之间的关系,加大了发生信息安全违规行为的可能性。

(2)信息安全意识对信息安全压力与道德推脱、道德推脱与信息安全违规意愿之间的关系有负向调节作用。说明员工的信息安全意识越高,信息安全压力对道德推脱的影响越弱,道德推脱与信息安全违规意愿之间的关系越弱。背后所隐含的内在逻辑是,员工对信息安全管理的重要性越熟悉,越知悉个人在日常工作中的信息安全职责,就越容易创造信息安全违规的屏蔽条件。这与D'ARCY et al.[49]和BULGURCU et al.[40]的研究结论一致,即员工信息安全意识越高,组织内部越不容易产生信息安全的违规行为。

(3)信息安全意识负向调节道德推脱在信息安全压力与信息安全违规意愿之间的中介作用,即员工信息安全意识越高,上述中介作用越弱,反之越强。也就是说,信息安全意识负向调节从信息安全压力到信息安全违规意愿的整个间接效应,即存在被调节的中介效应,而且这一被调节的中介效应通过信息安全压力与道德推脱和道德推脱与信息安全违规意愿之间关系的调节作用实现。这就意味着,信息安全压力可以通过道德推脱影响信息安全违规意愿,对于高信息安全意识的员工来说,这一影响过程和作用机制将会受到抑制。

本研究证实了信息安全压力除对信息安全违规意愿有直接的显著正向影响外,还通过道德推脱的中介机制间接影响违规意愿,信息安全意识对上述中介作用有完全的负向调节效应。在管理实践中,企业可以通过合理减轻员工的信息安全压力、提高员工的信息安全意识等手段减少员工信息安全违规行为的发生。

(1)减轻员工的信息安全压力。企业要求在工作中采用新的技术或系统,以及遵守既定的企业管理制度,往往会增加员工的心理压力[54]。在信息安全管理中,员工遵守信息安全管理制度,就会在原有工作的基础上增加工作负荷、复杂性和不确定性。因此,员工自觉执行信息安全管理制度的可能性就会下降。基于此,企业需要降低信息安全管理制度的复杂性,使员工不需要花费大量时间和精力完成系统的操作,从而加快工作进度。此外,企业的信息安全管理部门需要与员工有足够的沟通和反馈,以及时解决员工在信息安全管理中遇到的问题,减少工作中不清晰和不明确的地方。

(2)提高员工的信息安全意识。企业要明确信息资产和资源与企业的人力、物力和财力等同样重要,甚至在既定情况下企业信息资产的安全直接关乎企业的生存和发展,这样的理念应渗透并落实到员工的日常工作中。尤其是,需要以反面案例提醒员工信息安全违规行为的严重后果,如泄露企业客户的信息对客户造成的严重打击、没有及时修补企业系统漏洞引发的各种安全事故等。企业需要帮助员工明确和知晓信息安全违规行为造成的严重后果和伤害,这对于阻断员工违规行为的中和技术有重要作用,同样可以有效减少信息安全违规行为的发生。

(3)加强员工的职业道德培训。企业应开展或改善员工的信息安全意识培训,除了强调信息安全管理对于保护企业信息资产的重要性之外,还要突出强调遵守信息安全管理制度是员工职业道德素养的组成部分。与此相对应,员工才会在自我内在道德调节系统中深化遵守信息安全管理制度的必要性和重要性,有效抑制其信息安全违规行为的发生。同时,企业需要明确,员工信息安全意识的培养和提高不是一件一蹴而就的事情,需要在信息安全管理的方方面面有所体现,并且渗透到员工的日常工作中。只有这样,才能发挥信息安全意识的重要作用。

本研究仍存在不足和需要完善的地方。①为了保证量表的信度和效度,对研究模型中变量的测量均采用已有研究中被广泛使用和多次验证的题项。未来研究应该设计和开发更加符合中国企业信息安全管理情景的研究量表,以使研究结论更符合中国企业信息安全管理的实践。②问卷调查的对象均是中国通过信息安全管理体系认证的企业的内部员工,这在一定程度上限定了样本所属行业,而对信息安全管理要求较高行业的企业,往往注重信息安全管理体系的认证,导致研究样本覆盖的行业不够广泛,后续的研究应扩大样本量,以使研究结论更加具有代表性。

**参考文献:**

[1] POSEY C, ROBERTS T L, LOWRY P B, et al. Bridging the divide: a qualitative comparison of security thought patterns between information security professionals and ordinary organizational insiders. ***Information & Management***, 2014, 51(5): 551-567.

[2] POSEY C, ROBERTS T L, LOWRY P B. The impact of organizational commitment on insiders' motivation to protect organizational information assets. ***Journal of Management Information Systems***, 2015, 32(4): 179-214.

[3] JOHNSTON A C, WARKENTIN M, SIPONEN M. An enhanced fear appeal rhetorical framework: leveraging threats to

the human asset through sanctioning rhetoric. ***MIS Quarterly***, 2015,39(1):113-134.

[4] LEE Y. Understanding anti-plagiarism software adoption: an extended protection motivation theory perspective. ***Decision Support Systems***, 2011,50(2):361-369.

[5] LEE C, LEE C C, KIM S. Understanding information security stress: focusing on the type of information security compliance activity. ***Computers & Security***, 2016,59(1):60-70.

[6] CHENG L J, LI Y, LI W, et al. Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. ***Computers & Security***, 2013,39(Part B):447-459.

[7] D'ARCY J, HERATH T, SHOSS M K. Understanding employee responses to stressful information security requirements: a coping perspective. ***Journal of Management Information Systems***, 2014,31(2):285-318.

[8] CHEN Y, ZAHEDI F M. Individuals' internet security perceptions and behaviors: polycontextual contrasts between the United States and China. ***MIS Quarterly***, 2016,40(1):205-222.

[9] 陈昊,李文立,陈立荣. 组织控制与信息安全制度遵守:面子倾向的调节效应. **管理科学**, 2016,29(3):1-12.
CHEN Hao, LI Wenli, CHEN Lirong. Organization control and information security policy compliance: the moderating effect of face orientation. ***Journal of Management Science***, 2016,29(3):1-12. (in Chinese)

[10] HU Q, DINEV T, HART P, et al. Managing employee compliance with information security policies: the critical role of top management and organizational culture. ***Decision Sciences***, 2012,43(4):615-660.

[11] IFINEDO P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. ***Information & Management***, 2014,51(1):69-79.

[12] IFINEDO P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. ***Computers & Security***, 2012,31(1):83-95.

[13] VANCE A, SIPONEN M, PAHNILA S. Motivating IS security compliance: insights from habit and protection motivation theory. ***Information & Management***, 2012,49(3/4):190-198.

[14] 甄杰,谢宗晓,李康宏,等. 组织内部员工的信息安全保护行为:基于PMT和FAK整合视角的多案例研究. **管理案例研究与评论**, 2017,10(2):114-130.
ZHEN Jie, XIE Zongxiao, LI Kanghong, et al. Organization insiders' protection behaviors on information security: a multi-case study based on PMT and FAK. ***Journal of Management Case Studies***, 2017,10(2):114-130. (in Chinese)

[15] D'ARCY J, HERATH T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. ***European Journal of Information Systems***, 2011,20(6):643-658.

[16] IFINEDO P. Critical times for organizations: what should be done to curb workers' noncompliance with IS security policy guidelines?. ***Information Systems Management***, 2016, 33(1):30-41.

[17] 林润辉,谢宗晓,吴波,等. 处罚对信息安全策略遵守的影响研究:威慑理论与理性选择理论的整合视角. **南开管理评论**, 2015,18(4):151-160.
LIN Runhui, XIE Zongxiao, WU Bo, et al. The effect of sanction on information security policy compliance: an integrated framework based on DT and RCT. ***Nankai Business Review***, 2015,18(4):151-160. (in Chinese)

[18] SIPONEN M, VANCE A. Neutralization: new insights into the problem of employee systems security policy violations. ***MIS Quarterly***, 2010,34(3):487-502.

[19] LAZARUS R S. Coping theory and research: past, present, and future. ***Psychosomatic Medicine***, 1993,55(3):234-247.

[20] 王震,宋萌. 员工反馈规避行为的形成与后果:基于应对理论的实证研究. **科研管理**, 2015,36(5):127-138.
WANG Zhen, SONG Meng. The antecedents and consequences of employee feedback avoidance behavior from the perspective of a coping theory. ***Science Research Management***, 2015,36(5):127-138. (in Chinese)

[21] PEARSALL M J, ELLIS A P J, STEIN J H. Coping with challenge and hindrance stressors in teams: behavioral, cognitive, and affective outcomes. ***Organizational Behavior and Human Decision Processes***, 2009,109(1):18-28.

[22] BEAUDRY A, PINSONNEAULT A. Understanding user responses to information technology: a coping model of user adaptation. ***MIS Quarterly***, 2005,29(3):493-524.

[23] LIANG H G, XUE Y J. Avoidance of information technology threats: a theoretical perspective. ***MIS Quarterly***, 2009, 33(1):71-90.

[24] FADEL K J, BROWN S A. Information systems appraisal and coping: the role of user perceptions. ***Communications of the Association for Information Systems***, 2010, 26(1): 107-126.

[25] HERATH T, RAO H R. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. ***Decision Support Systems***, 2009, 47(2):154-165.

[26] BANDURA A. Social foundations of thought and action: a social cognitive theory. ***Journal of Applied Psychology***, 1986, 12(1):169.

[27] BANDURA A. Selective moral disengagement in the exercise of moral agency. ***Journal of Moral Education***, 2002, 31(2):101-119.

[28] BANDURA A. Moral disengagement in the perpetration of inhumanities. ***Personality and Social Psychology Review***, 1999,3(3):193-209.

[29] 文鹏,陈诚. 非伦理行为的"近墨者黑"效应:道德推脱的中介过程与个体特质的作用. **华中师范大学学报(人文社会科学版)**, 2016,55(4):169-176.
WEN Peng, CHEN Cheng. "Monkey see, monkey do" of unethical behaviors: the mediating role of moral disengagement and the moderating process of individual characteristics. ***Journal of Central China Normal University (Humanities and Social Sciences)***, 2016,55(4):169-176. (in Chinese)

[30] 赵红丹,周君. 企业伪善、道德推脱与亲组织非伦理行为:有调节的中介效应. **外国经济与管理**, 2017, 39

(1):15-28.
ZHAO Hongdan, ZHOU Jun. Corporate hypocrisy, moral disengagement and unethical pro-organizational behavior: moderated mediating effect. ***Foreign Economics & Management***, 2017,39(1):15-28. (in Chinese)

[31] 张艳清,王晓晖,王海波.组织情境下的不道德行为现象:来自道德推脱理论的解释.**心理科学进展**,2016,24(7):1107-1117.
ZHANG Yanqing, WANG Xiaohui, WANG Haibo. Unethical behaviors in organizational context: the explanation from moral disengagement theory. ***Advances in Psychological Science***, 2016,24(7):1107-1117. (in Chinese)

[32] MOORE C, DETERT J R, TREVINO L K, et al. Why employees do bad things: moral disengagement and unethical organizational behavior. ***Personnel Psychology***, 2012,65(1):1-48.

[33] HANNAH D, ROBERTSON K. Why and how do employees break and bend confidential information protection rules?. ***Journal of Management Studies***, 2015,52(3):381-413.

[34] BARSKY A. Investigating the effects of moral disengagement and participation on unethical work behavior. ***Journal of Business Ethics***, 2011,104(1):59-75.

[35] REZGUI Y, MARKS A. Information security awareness in higher education: an exploratory study. ***Computers & Security***, 2008,27(7/8):241-253.

[36] HERATH T, RAO H R. Protection motivation and deterrence: a framework for security policy compliance in organizations. ***European Journal of Information Systems***, 2009,18(2):106-125.

[37] SMITH S, WINCHESTER D, BUNKER D, et al. Circuits of power: a study of mandated compliance to an information systems security de jure standard in a government organization. ***MIS Quarterly***, 2010,34(3):463-486.

[38] CROSSLER R E, JOHNSTON A C, LOWRY P B, et al. Future directions for behavioral information security research. ***Computers & Security***, 2013,32(1):90-101.

[39] 武德昆,官海滨,王兴起,等.高管支持对信息安全管理有效性的影响研究:信息安全意识的中介效应.**中国海洋大学学报(社会科学版)**,2014(2):44-50.
WU Dekun, GUAN Haibin, WANG Xingqi, et al. The influence of top management support on the effectiveness of information security management: mediating effect of information security awareness. ***Journal of Ocean University of China (Social Sciences)***, 2014(2):44-50. (in Chinese)

[40] BULGURCU B, CAVUSOGLU H, BENBASAT I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. ***MIS Quarterly***, 2010,34(3):523-548.

[41] DINEV T, HU Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. ***Journal of the Association for Information Systems***, 2007,8(7):386-408.

[42] PUHAKAINEN P, SIPONEN M. Improving employees' compliance through information systems security training: an action research study. ***MIS Quarterly***, 2010,34(4):757-778.

[43] 谢宗晓,林润辉,王兴起.用户参与对信息安全管理有效性的影响:多重中介方法.**管理科学**,2013,26(3):65-76.
XIE Zongxiao, LIN Runhui, WANG Xingqi. Impact of user participation on the effectiveness of information security management: the multiple mediation approach. ***Journal of Management Science***, 2013,26(3):65-76. (in Chinese)

[44] MYYRY L, SIPONEN M, PAHNILA S, et al. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. ***European Journal of Information Systems***, 2009,18(2):126-139.

[45] SIPONEN M T. A conceptual foundation for organizational information security awareness. ***Information Management & Computer Security***, 2013,8(1):31-41.

[46] KRUGER H A, KEARNEY W D. A prototype for assessing information security awareness. ***Computers & Security***, 2006,25(4):289-296.

[47] DETERT J R, TREVINO L K, SWEITZER V L. Moral disengagement in ethical decision making: a study of antecedents and outcomes. ***Journal of Applied Psychology***, 2008, 93(2):374-391.

[48] SPEARS J L, BARKI H. User participation in information systems security risk management. ***MIS Quarterly***, 2010,34(3):503-522.

[49] D'ARCY J, HOVAV A, GALLETTA D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. ***Information Systems Research***, 2009,20(1):79-88.

[50] 周浩,龙立荣.共同方法偏差的统计检验与控制方法.**心理科学进展**,2004,12(6):942-950.
ZHOU Hao, LONG Lirong. Statistical remedies for common method biases. ***Advances in Psychological Science***, 2004,12(6):942-950. (in Chinese)

[51] EDWARDS J R, LAMBERT L S. Methods for integrating moderation and mediation: a general analytical framework using moderated path analysis. ***Psychological Methods***, 2007,12(1):1-22.

[52] 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. (in Chinese)

[53] 方杰,温忠麟,张敏强,等.基于结构方程模型的多重中介效应分析.**心理科学**,2014,37(3):735-741.
FANG Jie, WEN Zhonglin, ZHANG Minqiang, et al. The analyses of multiple mediation effects based on structural equation modeling. ***Journal of Psychological Science***, 2014,37(3):735-741. (in Chinese)

[54] AYYAGARI R, GROVER V, PURVIS R. Technostress: technological antecedents and implications. ***MIS Quarterly***, 2011,35(4):831-858.

# Information Security Stress and Employees' Violation Intention: Moderated Mediation Effects

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

1 School of Business Planning, Chongqing Technology and Business University, Chongqing 400067, China

2 Department of Information Security Service, China Financial Certification Authority, Beijing 100054, China

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

**Abstract**: It has been continuously proved that adoption of information technology and information systems has a positive effect on organizational performance. Thus, information resources have become important assets, which are related to the survival and development of organizations. However, employees' violations of organizational information security policies, whether intentional or unintentional, often put the organization at great risk even leading to disastrous losses. As such, employees' violations of organizational information security policies are viewed as the insider major concern in organizational information security management. Previous studies have investigated influencing factor of employee violations of information security policies, however, the existing research has not yet formed a unified conclusion and disengages from the practice of organizational information security management. Therefore, these studies failed to offer organization targeted suggestions on how to reduce employees' information security violations.

Based on coping theory and moral disengagement theory, this study explores the influence mechanism of information security stress to employees' information security violation intention using a moderated mediation model. That is, moral disengagement is the mediating variable, so well as information security awareness is the moderating variable. A survey was conducted on the organizations which has passed the information security management system (ISO/IEC 27001). 318 valid samples were obtained, and the hypotheses were tested by multiple liner regression and moderated path analysis methods.

The results indicated that: ① information security stress has a significant positive effect on information security violation intention, and moral disengagement is the mediating variable between information security stress and employee's information security violation intention; ② information security awareness has a negative moderating effect on the relation between information security stress and moral disengagement, as well as the relation between moral disengagement and information security violation intention; ③ information security awareness has a negative moderating effect on the mediating effect of moral disengagement on information security stress and information security violation intention. Thus, there exist mediated mediation effects. In other words, the higher the information security awareness is, the weaker mediating effect and vice versa.

The results of this study clarify the influence mechanism of information security stress to employee violation intention of organizational information security policies, deepen the understanding of employee information security stress, and enrich the theoretical research of behavioral information security management. In addition, the current study also provides some implications for organizations on how to effectively control and reduce employee information security violations through improving employee information security awareness and strengthening employee professional ethics training.

**Keywords**: information security stress; information security awareness; violation intention; moral disengagement; coping theory

**Received Date**: July 5th, 2017 **Accepted Date**: March 21st, 2018

**Funded Project**: Supported by the National Natural Science Foundation of China (71672123), the Chongqing Basic Science and Frontier Technology Research Project (cstc2017jcyjAX0441), the Chongqing Social Science Planning Project (2017QNGL55), the Humanities and Social Science Research Project of Chongqing Municipal Education Commission (17SKG097) and the Research Project of Chongqing Technology and Business University (1751030)

**Biography**: ZHEN Jie, doctor in management, is a lecturer in the School of Business Planning at Chongqing Technology and Business University. His research interests include behavior of information security and e-commerce. His representative paper titled "Research on factors influencing intention to personalize product online based on theory of planned behavior" was published in the ***Forecasting*** (Issue 6, 2016). E-mail: zhenjie886@163.com

XIE Zongxiao, doctor in management, is the manager of Department of Information Security Service at China Financial Certification Authority. His research interest focuses on cyber and information security management. His representative paper titled "Institutional pressures, information security legitimation and organizational performance: an empirical study based on Chinese enterprises" was published in the ***Management World*** (Issue 2, 2016). E-mail: xiezongxiao@vip.163.com

DONG Kunxiang, doctor in management, is a lecturer in the School of Management Science and Engineering at Shandong University of Finance and Economics. His research interests include information security risk management and crowdsourcing. His representative paper titled "Factors affecting innovation performance of solvers in crowdsourcing contest: the moderating role of perceived risk" was published in the ***Science of Science and Management of S.& T.*** (Issue 2, 2016). E-mail: dkxgood@163.com □