组织员工信息系统安全行为研究进展

陈昊，李文立，柯育龙

（大连理工大学 管理与经济学部,辽宁 大连 116023）

摘 要 组织员工的信息安全行为是保障组织信息资产安全的重要前提，而现有国内组织情境下的信息安全研究缺少基于行为视角的系统化探讨。本文致力于梳理现有研究中影响组织员工从事信息安全行为的关键要素。针对信息系统安全政策遵从行为和违背行为，在整合主要理论和解释关键结论差异的基础上，从“需求与控制”视角和“自我管理”视角构建组织员工信息系统安全行为的理论研究框架。同时，阐明了信息安全行为研究未来可能的研究方向。

关键词 信息安全，信息系统安全政策，遵从行为，违规行为，信息安全行为管理

中图分类号 C931.6

1 引言

信息技术（Information Technology, IT）的商业价值及其对组织绩效的贡献毋庸置疑[1]，越来越多的企业采用信息系统（Information System，IS）来优化业务流程和提升工作绩效。然而 IS 的不正确使用和外部入侵也使组织承受着信息资产泄露的巨大风险。据 2013 年调查数据显示，93%的英国大型企业曾发生过信息安全事件，导致的平均损失已经达到 45-85 万英镑[2]。安装防火墙，更新杀毒软件，设置监控系统和使用防护密码等信息安全防护技术和措施，虽然能在一定程度上保护企业的信息资源安全，但是组织员工不正确的使用习惯，对信息系统的滥用和误用行为等都无法通过技术手段来解决[3, 4]。2013 年调查数据显示，74%的信息安全事件与内部员工相关[5]，组织员工的内部威胁已经超越外部威胁成为信息安全事件的首要诱因[6]。内部员工对组织信息资产造成的直接或间接的威胁行为有两类：故意行为（如破坏、偷窃组织信息，以及商业间谍行为等）和无意行为（如设置较为简单的密码，粗心点击了含有钓鱼链接的邮件等）[7]，且无论是哪种行为，因内部人员的不恰当行为给企业组织造成的损失都是灾难性的。

企业高层推行安全教育培训和意识项目（Security Education, Training, and Awareness，SETA）以及信息系统安全政策（Information System Security Policies，ISSP）来规范员工的信息系统安全行为已被广泛应用于企业实践。安全教育培训和意识项目致力于强化员工的信息安全意识，并明确员工对于威慑严厉性和确定性的认知[8]，从而提升用户遵从信息系统安全政策的意愿和安全解决方案的使用[9]。信息系统安全政策则以正式制度的形式表明了组织对于信息安全的立场和态度，是安全决策制定和实施的基础[10]。虽然企业从技术，管理和流程等多方面措施来维护组织的信息系统安全，但是信息系统安全事件依然层出不穷，究其原因还是员工在信息系统的使用过程中，对信息系统安全政策有意或者无意的违背行为所造成。

基金项目：国家自然科学基金项目：员工信息安全违规意愿的社会控制要素及实证研究(71272092)

通讯作者：陈昊，大连理工大学管理与经济学部，博士研究生。E-mail: ch9569@mail.dlut.edu.cn

近年来，针对员工信息系统安全行为（Information System Security Behavior）的探讨是国外信息系统行为研究领域的热点，尤其是借鉴犯罪学、社会心理学、健康学和组织行为学等领域的理论，对组织员工的计算机/信息系统滥用和误用行为（Computer/Information System Abuse and Misuse）、信息系统安全政策的遵从与违背行为（Information System Security Policy Compliance and Violation Behavior）、信息安全保障行为（Information Security Assurance Behavior）和信息安全疏漏行为（Information Security Omission Behavior/ Knowing-doing Gap）等主题进行了深入探讨。尽管现有研究取得了丰富的成果，然而多数研究停留在变量关系的验证以及外来理论在信息安全研究中的适配度的验证，尚未形成较为完整的理解组织情境下员工信息安全行为研究的清晰理论体系。此外，国外研究的很多结论具有较强的研究情境依赖性，即便是同一主题下基于相同理论的研究结论仍然存在差异甚至矛盾。同时，有关信息安全行为学视角的探讨在国内尚未引起过多关注，缺乏针对组织员工信息安全行为的系统化研究。本文在回顾国内外相关文献的基础上，梳理影响员工信息系统安全政策遵从行为和违背行为的关键影响要素，明确各要素之间的作用机理，并对相关结论的差异进行归纳和解释，构建组织情境的员工信息系统安全政策遵从和违背行为的研究框架。希望本文对国内外研究文献的综述，能够对基于行为学研究视角的信息安全研究的开展提供借鉴，力求为后续研究提供理论基础和发展方向。另外，本研究有助于企业了解员工的信息安全行为动机，为组织信息系统安全政策与控制措施的制定和实施提供理论依据，同时为员工信息安全实践的引导和规范，以及违规行为的预防提供实践指导。

2 研究方法与过程

2.1 概念界定

信息安全行为领域的研究针对安全相关的行为现象并未形成统一的分类标准[11, 12]，很多行为之间存在着概念上的交叉和涵义上的混淆，造成了现有研究结论的不一致甚至相悖。本研究的主要目的致力于发现和揭示影响组织员工信息安全行为的关键要素，而非针对各类安全相关行为的分类学探讨。根据已有文献认为信息系统安全政策遵从行为和违背行为并非是完全对立的两种行为[11]，很多用来解释遵从行为的因素并不能用于揭示违规行为的作用路径，就像 IS 成功的关键要素与 IS 失败的关键因素不同一样。因此为了更清晰的突出研究主题，本文归纳性地将组织情境下员工的信息安全行为划分为两类：信息系统安全政策遵从行为和信息系统安全政策违背行为。并将现有研究中出现频率较高的四类消极行为---计算机（或信息系统）滥用/误用、不道德的计算机使用、非恶意安全违规行为和信息安全疏漏行为---统一归类为信息系统安全政策违背行为。行为定义及示例如表 1 所示。

表 1 信息安全行为定义与归类

行为		涵义	示例
信息系统安全政策遵从行为		员工在日常工作中按照组织信息系统安全政策的规定使用信息系统和组织信息资源的行为	设置强密码、定期更新安全补丁、使用安全防护软件等
信	指员工忽视	员工非授权的或故意的滥用组织信息	如使用盗版软件、非

信息系统安全政策违背行为：或违反信息安全政策所导致的行为。该行为可能是员工的意识性行为或无意行为，对信息资产安全带来实际损失或潜在性风险。	信息系统（计算机）滥用/误用行为	系统资源(如软硬件\数据和计算机服务等)的行为	法访问数据、未授权的修改数据等
	信息安全疏漏行为	员工意识到信息安全风险但还是选择无视信息安全政策的行为	从未更换密码；不升级系统补丁；不进行备份数据等
	非恶意的违规行为	员工出于非主观恶意的目的进行为违规行为	在便签上记录密码；拷贝敏感数据回家工作等
	计算机不道德使用	员工对计算机或者信息系统的不恰当的使用行为	未经授权拷贝软件和数据等

注：根据 Guo（2013）[11]的研究整理和修改

2.2 文献检索

对管理科学和信息系统研究领域的 Business Source Premier （EBSCO）、Web of Science 和 Elsevier（Science Direct）和 Emerald 数据库进行检索，检索领域包括题目、摘要和关键字，检索条件为学术期刊类型，文献类型选择全文文章，检索时间限定为 2000 年 1 月-2014 年 12 月。检索关键词组合与结果详见表 2。通过对研究主题的筛选与阅读，清除重复和无效记录后得到 70 篇密切相关的有效论文。

表 2 国外期刊文献检索结果

检索条件组合 / 数据库名称	End-users *OR* Organization Staff *OR* Employees		
	AND		
	Information System Security Policy		Computer OR Internet OR Information System
	AND		*AND*
	Compliance Behavior *OR* Adherence *OR* Follow	Violation *OR* Non-compliance Behavior *OR* Omission Behavior	Misuse *OR* Abuse *OR* Unethical use
EBSCO	7	5	9
Elsevier	22	20	9
Web of Science	18	9	7
Emerald	8	--	5
筛选后结果	31	22	17

国内有关于组织情境下的信息安全行为研究方兴未艾。截止到 2014 年底，以“信息安全行为”为关键字对中国知网、万方和维普三大中文文献数据库进行检索，筛选出涉及组织情境下员工信息安全行为研究的博硕士学位论文 9 篇，涉及组织情境下信息安全管理的博硕士论文 4 篇[13-16]。然而仅发现个别期刊文献涉及组织情境下员工信息安全行为研究，其中曾忠平等对信息安全行为中的人因风险进行了归纳梳理[17, 18]。国内行为学视角的信息安全行为研究主题详见表 3。通过梳理发现国内针对组织情境下员工信息安全行为管理的研究尚处于起步阶段，已有研究多采用案例研究方法和实证研究方法针对安全行为的分类、信息安全政策的遵从与违规行为、互联网使用行为的主题进行了探讨。

表 3 基于行为学视角的国内信息安全研究文献归纳

作者	理论基础	研究情境	关键结论（或贡献）	研究方法
翁勇南[19]	-----	员工的信息安全行为	构建潜在内部威胁者行为模型以及企业内部威胁因素模型，设计针对国内组织的内部信息安全管理情况及影响组织内部信息安全的个人行为因素及环境因素的调查问卷	案例分析
常建轩[20]	-----	政策遵从行为和参与行为	从策略本身特质、社会环境因素和员工个人因素三个方面选取相关变量，提出衡量信息安全策略实施效果的定量方法	实证研究
李瀛[21]	威慑理论 社会纽带理论	员工信息安全违规行为	社会纽带(依恋、承诺、参与和信念)和社会压力对员工的违规意愿均有显著的影响；惩罚严厉性对员工的信息安全违规意愿有显著的抑制作用，惩罚确定性的影响并不显著	实证研究
陈琳[22]	社会认知理论 大众威慑理论	员工信息安全政策遵从行为	员工的自我效能、与个人相关结果预期和感知惩罚的严重性对遵从信息安全政策有显著影响；员工的与组织相关的结果预期和感知惩罚的确定性则对遵从行为的影响不显著	实证研究
李科[23]	复合行为模型	互联网不当使用行为	工作绩效期望、工作组规范和互联网不当使用行为态度对员工的互联网不当使用行为意向有显著影响	实证研究
石栩楠[24]	计划行为理论 威慑理论	企业员工的信息系统安全行为	正式约束和非正式约束与实际行为之间存在正向影响且影响显著，羞耻对实际行为影响不显著，对信息系统安全中个人的实际行为无明显作用	实证研究
程丽娇[25]	中和技术理论 理性选择理论	员工互联网滥用行为	中和技术策略、感知的安全隐患和感知的收益均显著的影响员工的互联网滥用意愿；然而感知的惩罚严重性和惩罚确定性的影响作用不显著	实证研究
袁园园[26]	理性选择理论	员工互联网使用策略遵从行为	员工的互联网使用策略遵从意向受到自我规范和自我效能的影响，感知遵从互联网使用策略行为的利益和不遵从互联网使用策略行为的代价对员工的遵从意向产生促进作用	实证研究
王冬梅[27]	理性选择理论 中和技术理论 组织环境要素	员工信息安全违规行为	感知收益、感知惩罚确定性、中和技术、同事偏差行为影响员工的信息安全违背意图；感知惩罚严重性在个人道德信念和自我控制的调解下负向显著影响信息安全违背意图	实证研究

注：作者整理

2.3 研究框架

现有文献从“需求与控制”（Command-and-Control Approach）和“自我管理”（Self-regulatory Approach）两个层面来探讨组织员工的信息安全行为决策。“需求与控制”层面强调外部动机，认为员工对组织规章制度的畏惧心理以及对威胁和成本等的恐惧心理是其实施信息安全行为的重要动力。“自我管理”层面则看重员工的内部动机，认为员工内心的渴望或道德价值观等的自我驱使是实施信息安全行为的关键力量。本文拟基于上述理论框架对现有文献涉及到的关键理论和研究结论进行回顾和整理，从而揭示对组织员工的信息系统安全政策遵从行为和违背行为的关键影响因素。根据与有文献的研究结论构建如图 1 所示的综述分析框架。

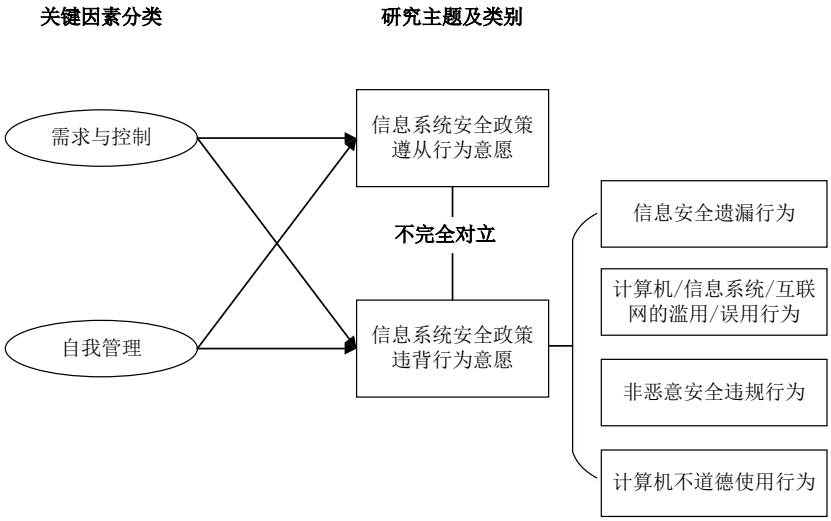

图 1 综述分析框架

3“需求与控制”视角下的信息安全行为

3.1 威慑理论

犯罪学领域的威慑理论（Deterrence Theory）认为通过惩罚的确定性（Certainty of Sanction）、惩罚的严厉性（Severity of Sanction）和惩罚的及时性（Celerity of Sanction）进行控制和管理人的行为，因为没有人希望受到惩罚[28]。也就是说，一旦人们认识到从事不被组织认可的行为受到惩罚的可能性较大、力度较强，以及/或者组织会对实施这种行为的员工做出及时的处罚响应时，他们将倾向于放弃实施这种行为转而从事符合组织要求的行为。信息安全行为研究更多关注于威慑的确定性和威慑的严厉性。惩罚的公平性同样重要，员工感知到的惩罚越公平，越能驱动他们遵从信息系统安全政策[29]。此外，还有研究采用扩展的威慑理论，从正式威慑（Formal Sanction，包含威慑的确定性和严厉性）、非正式威慑（Informal Sanction）和羞愧（Shame）的角度开展研究[30, 31]。

已有文献对于组织威慑的研究存在争议，争议主要有三个方面：（1）威慑本身的含义。信息安全行为研究领域认为威慑与惩罚（Punishment）、惩处（Penalty）和监控（Detection）含义相近，很多研究将上述术语交替使用；（2）威慑维度的构成。基于扩展的威慑理论的研究对于非正式威慑含义的认识并不统一。Siponen 等[30]和 Vance 等[31]的研究均认为非正式威慑是朋友或同事伙伴对于指定行为的不赞同所带来的影响，而 Hovav 等[32]则直接将道德信念等同于非正式威慑。此外，Guo 等[33]的研究从组织威慑、工作组威慑和自我威慑三个层面对威慑进行了重新定义。（3）即便是相同研究情境下的研究结论同样存在争议。如 Herath 等[4, 34]发现仅有员工感知到的威慑的确定性对信息系统安全政策的遵从行为产生正向影响作用，而感知到的威慑的严厉性不起作用。Son[35]的研究则认为感知到的威慑的可能性和严厉性对信息系统安全政策遵从行为均不产生任何作用。

表 4 归纳了信息系统安全行为研究领域涉及组织威慑的主要研究结论。研究结论的差异表明组织威慑对于员工的信息安全行为并非实时有效[36]，很大程度上依赖于研究情境[37]、个人的道德水平[28, 38]和行为取向[30, 39]。D`Arcy 等[28]还认为计算机自我效能、自我控制（Self-control）等个人因素，以及虚拟状态（Virtual Status）和员工职位（Employee

Position）等情境因素是造成研究结论差异的重要原因。尽管如此，威慑机制依然被认为是组织正式控制的重要组成内容[40, 41]，探讨如何发挥组织威慑的关键性作用成为当前研究的热点。比如 Liang 等[41]基于调节定向理论（Regulatory Focus Theory）认为个人的行为取向与趋利避害的动机相关，发现着眼于预防为主的人对失败、损失和惩罚非常敏感，由此为了避免可能的惩罚，他们会选择遵从。Siponen 等[30]和 Cheng 等[42]发现威慑对使用中和技术（Neutralization Technologies）的员工失效，员工可以通过使用否认责任、否认伤害等中和技术进行辩解，以逃避组织处罚。Hu 等[39]则认为一旦从事违规行为带来的收益大于组织威慑产生的成本的话，人们将违背信息安全行为。

表 4 基于威慑和惩罚的主要研究结论及差异

来源	基本构念	关键结论
信息系统安全政策遵从行为情境下的研究结论：		
Jai-Yeol [35]	感知到的威慑确定性、感知到的威慑严厉性	未发现两者与信息系统安全政策遵从意愿之间的关系
Herath 等[4, 34]	处罚严厉性、监控确定性	处罚严厉性负向影响信息系统安全政策遵从意愿 监控确定性正向影响信息系统安全政策遵从意愿
Xue 等[29]	惩罚期望、惩罚公平性	惩罚公平性正向影响 IT 遵从意图 未发现惩罚期望与 IT 遵从意图间的关系
Chen 等[40]	威慑严厉性	威慑的严厉性正向影响信息系统安全政策遵从意愿
Liang 等[41]	惩罚期望	惩罚期望正向显著影响员工的 IT 遵从行为
Li 等[38, 43]	威慑严厉性、监控可能性	监控确定性正向影响互联网安全政策遵从意愿 未发现处罚严厉性与互联网安全政策遵从意愿间的关系
信息系统安全政策违背行为情境下的研究结论：		
Siponen 等[30]	正式威慑、非正式威慑、羞愧	引入中和技术理论后，未发现三个构念与信息系统安全政策违背意愿之间的关系
Hu 等[39]	威慑严厉性、威慑确定性、威慑及时性	未发现二阶变量（威慑）和各一阶变量与计算机系统政策违背意愿之间的关系
Guo 等[44]	感知到的威慑	未发现感知到的威慑与非恶意安全违背态度间的关系
D`Arcy 等[37]	威慑的严厉性、威慑的确定性	未证实威慑的确定性与信息系统误用意愿之间的关系 威慑的严厉性负向影响信息系统误用意愿
Vance 等[31]	正式威慑、非正式威慑	非正式控制负向影响信息系统安全政策违背意愿 未发现正式威慑与信息系统安全政策违背意愿间关系
Hovav 等[32]	威慑严厉性、威慑确定性 非正式威慑（道德信念）	美国情境下威慑严厉性负向显著影响信息系统误用意图，未发现威慑确定性与信息系统误用意图之间的关系 韩国情境下威慑确定性负向显著影响信息系统误用意图，未发现威慑严厉性与信息系统误用意图之间的关系 两文化情境：非正式威慑负向影响信息系统误用意图
Guo 等[33]	组织威慑、工作组威慑、自我威慑	工作组威慑和自我威慑均负向影响违背信息安全政策意愿；未证实组织威慑与违背信息安全政策意愿间的关系

注：作者整理

3.2 理性选择理论

理性选择理论（Rational Choice Theory）是有关于人们如何平衡利益和成本以做出适

合的决策的理论。理性选择理论被广泛应用于犯罪学研究领域，认为一旦从事犯罪行为获得的期望利益远大于实施成本，那么犯罪行为将会发生。信息安全行为研究往往将组织威慑被认为是一种成本，而奖励（实施违规行为所取得的收益）则被看作是一种收益。奖励机制作为组织正式控制方式能有效培育员工的行为动机和绩效[40]，一旦员工从事了组织既定的行为或者达成了组织期望的结果，那么员工将受到奖励[45]。奖励措施实施的重要效果之一就是增加了政策的强制性[46]。如果制定了信息安全政策而没有采取相应的奖励措施来激励员工遵从，那么员工会认为这些政策并没有那么重要或者缺乏强制性。研究证实奖励能有效增加员工的感知到的利益，进而影响员工遵从信息安全行为的态度[47]。

基于理性选择理论的研究发现即便是具有一定的道德信念的员工，如果他们认为从事违规行为的收益大于成本的话，他们将倾向于从事违规行为，组织威慑的作用将失效[31]。反之，如果遵从信息系统安全政策的收益远大于由安全风险和组织控制机制产生的不遵从成本的话，员工会倾向于选择遵从信息系统安全政策[38]。Bulgurcu 等[47]认为除了遵从收益和不遵从成本，员工遵从信息系统安全政策有可能会给工作带来一些不便（比如有的员工按照政策规定使用强密码从而增加了记忆难度），由此产生的遵从成本也应该考虑在内。研究认为遵从利得、不遵从成本和遵从成本共同影响员工的遵从态度。Li 等[38]则证实不遵从行为所取得的收益（如工作时间从事非工作上网行为等）对信息系统安全政策遵从行为产生负向影响。Ng 等[48]发现感知到的利益对员工的计算机安全行为起正向预测作用。

3.3 保护动机理论

保护动机理论（Protection Motivation Theory)[49]提供了一个清晰的框架用以揭示恐惧诉求对个人生成保护动机所产生的影响作用。保护动机理论的主体框架包含两个部分：威胁评估和效用评估。个人之所以采取应对措施是基于威胁评估和效用评估的结果[34]。实质上保护动机理论是基于理性计算的认知过程，威胁评估包括对威胁可能性和严重性的判断（感知易损性和感知严重性），以及不采取措施或者继续经历这种风险可能会带来的好处的感知（收益）；效用评估则包括对哪种响应可以有效减少或者避免这种威胁的认知（响应有效性），以及应对这种威胁所需要的能力的认知（自我效能），当然还包括对响应这些措施或能力所耗费的成本认知（响应成本）。保护动机理论适合于探讨风险相关的行为，实证发现威胁评估和应对评估能够显著影响员工遵从信息系统安全政策的意愿[50, 51]。具体来讲，感知易损性、感知严重性、响应有效性和自我效能对员工的信息系统安全政策遵从行为有正向显著影响，而收益和响应成本则产生负向影响作用[52]。Ifinedo[50]的研究结论则认为感知严重性对员工的信息安全遵从行为起负向作用，响应成本则不起作用，这可能是样本量的差异和外部影响等差异造成的。此外，Vance 等[52]的研究还发现习惯会影响员工对威胁和应对的评估认知过程，是影响个人认知的重要前因变量。

自我效能（Self-efficacy）也经常被单独探讨。作为社会认知理论中的重要概念，自我效能在信息安全行为领域用来评估个人从事信息安全行为所具备的知识、技能、资源（如时间金钱）等条件和能力。研究发现，计算机使用经验的积累和对风险可控性的认知能促进员工自我效能的增长，自我效能感高的员工容易从事安全实践行为[53]和采取安全预防措施[45]，他们愿意为维护信息资产安全而努力[53]，并倾向于保护组织隐私[54]和遵从信息系统安全政策[53, 55]。

3.4 组织行为学相关理论与关键要素

（1）非正式控制：社会规范

社会规范（Social Norm，或社会影响 Social Influence[56]）被定义为一种被一群人所接受的用来引导和/或规范社会行为的规范或者标准，它没有法律的强制力[57]。已有文献探讨过四种类型的社会规范：指令性规范（Injunctive Norm）、示范性规范（Descriptive Norm）、主观规范（Subjective Norm）和个人规范（Personal Norm）。其中，个人规范实质上就是个人的道德义务[38, 57]，本文将在个人属性因素中进行阐述。

指令性规范是指在给定的情境下个人对于周围大多数人对某行为赞成与否的感知；而示范性规范则是在给定的情境下个人对于他人如何行动的感知。指令性规范和示范性规范被证实能有效解释组织员工的信息系统安全政策遵从行为意图，解释度达到 65%[58]。此外，他人影响（Peer Influence）或者工作组规范（Workgroup Norm）也是文献中经常提及的概念，该概念与示范性规范的概念含义相近[34]，指代个人从事某行为与否取决于他仿照周围他人行事的倾向。社会学习理论认为人们会通过观察模仿来学习彼此的行为，并在这个过程中产生一种社会压力迫使人们从事一致性的行为。人们总是会参照周围可见的一些惯例做法来行事，一旦大多数的重要他人都开始或者倾向于遵从信息系统安全政策的话，那么员工也会做出相同的响应。已有文献大量证实他人影响对于信息系统安全政策遵从行为呈显著正向相关关系[4, 34]，并且工作组规范对员工从事非恶意违规行为的态度有正向导向作用[44]。

主观规范是在特定情境下个人是否执行某行为时感知到的来自重要他人的社会压力。一般情况下，主观规范会被默认为是一种符合组织利益的或者与组织既定目标具有一致性的一种认知。比如如果周围的同事均从事信息安全行为的话，那么其他人也会仿照从事相同的行为。主观规范的建立依赖于规范信念，基于 TPB 或 TRA 理论框架的研究普遍证实主观规范能有效预测和解释员工的信息系统安全政策遵从行为意愿。然而，也有研究没有发现主观规范与遵从行为之间的关系[59]，并预测这可能与组织中业已形成的负向规范（如互联网滥用习惯）有关。Dugo [60]的研究则进一步证实从事信息系统安全政策违背行为的主观规范越强烈，员工越倾向于产生违规意愿。但是到目前为止，这种负向规范（或者习惯）并没有引起研究者的重视，有关于负向规范对信息系统安全政策违背行为的诱导作用尚未证实。

（2）组织文化与安全氛围

组织文化通过塑造员工价值观和加强组织承诺来引导员工从事符合组织期望的行为[61]。已有文献证实良好的组织文化对员工的信息系统安全政策遵从行为有直接的正向影响作用。Chang 等[62]将组织文化划分为合作性、创新性、一致性和有效性四个维度，探讨组织文化与信息安全管理行为的关系。结果发现灵活性的文化（创新性和合作性）与信息安全测度呈负相关或无关；而控制性文化（一致性和有效性）对信息安全的测度有显著的正向影响。D`Arcy 等[63]认为以高层管理承诺、安全沟通和计算机监控为重要内容的信息安全文化是员工实施信息系统安全政策遵从行为的前提。类似的，Chan 等[64]从同事交往、直接的监督和高层实践三个层面构建信息安全氛围，证实信息安全氛围对员工的信息系统安全政策遵从行为产生正向的显著影响。

高层管理者是推动组织文化构建的重要推手。Puhakainen 等[65]发现组织高层对信息安全行为的态度将显著影响员工对信息安全行为的态度，如果员工发现高层领导者对信息系统安全政策持消极态度，那么员工也会采取同样的应对方式并实施违规行为。而高层领导者态度的转变能大大提升员工遵从信息系统安全政策的态度和实践。Hu 等[61]认为高层管理者的参与是影响员工信息系统安全政策遵从行为的重要外部因素，是构建目标导向文化

和规则导向文化的重要前提，同时证实组织文化对员工遵从态度有显著的正向影响。

（3）工作相关认知要素

组织承诺（Organization Commitment）是员工对于组织的认同和涉入程度。组织承诺高的员工会以此为内在的规范压力，从而驱使自己实现组织目标和利益。已有文献证实高组织承诺的员工几乎不会从事信息系统的违规行为。由此，组织承诺越高的员工越会选择遵从组织的信息系统安全政策[34, 66, 67]。

工作满意度（Job Satisfaction）是员工与工作有关的情感反应。根据社会交换理论，如果员工认为自己的工作贡献能够被组织重视和受到期望中的对待，他们将乐意从事这种行为并使组织获利。由此，工作满意度高的员工倾向于遵从组织的信息系统安全政策[63, 66]。

组织支持感（Organization Support）是指员工感知到的组织对于员工个人贡献的价值的重视程度。组织支持感高的员工认为从事组织期望的行为将得到组织认可和奖励，由此员工愿意帮助组织达成目标并形成忠诚。然而，实证结果显示组织支持感却负向影响信息系统安全政策遵从行为[63]。类似地，Zhang 等[59]的研究同样发现组织提供的技术支持越完备，员工越容易对信息安全产生懈怠。

4 “自我管理”视角下的信息安全行为

4.1 道德与价值观

道德理性（Moral Reasoning）是个人使用道德准绳进行行动决策的过程。道德通过一系列的被公认的观念和准则来强化个人的义务与责任，从而纠正违规行为和选择从事正确的道德行为。道德理性或道德信念（Moral Beliefs）能有效降低员工的信息安全违规意愿[31]，被认为是解释员工信息系统安全政策遵从行为的重要因素[9, 68]。信息安全文献中经常使用个人规范（Personal Norm）指代个人从事某行为的道德标准。Li 等[38]发现个人规范能够有效控制组织员工遵从互联网使用政策的意愿，同时对威慑作用的效果起到调节作用。Myyry 等[69]采用六阶段道德判断标准将人的道德理性划分为道德成规前期（Preconventional Level）、成规期（Conventional Level）和道德成规后期（Postconventional Level）三个阶段。处在道德成规前期阶段的人多为青少年或者不成熟的成人群体，他们的行为往往从个人利益出发，有着明显的趋利避害特征；大多数成年群体处于成规期阶段，他们会以组织制定的规章制度作为行动标准以符合自己的社会角色；而处于道德成规后期的群体已经将遵从组织规章制度看作是一种内化的惯常性行为，他们会自觉地为组织考虑从而从事安全行为。实证结果发现只有道德成规前期的理性与信息系统安全政策遵从行为呈显著正相关关系。

道德信念同样是解释信息系统安全政策违背意愿的重要变量，研究认为人们之所以不愿意从事违规行为并非出于对于威慑的恐惧，而是从道德立场认识到这种行为的错误性。Hovav 等[32]通过在韩国和美国两种文化情境下的研究发现，道德信念作为一种非正式威慑能显著的抑制员工从事信息系统误用的意愿。Vance 等[31]的研究同样证实道德信念与员工的信息系统安全政策违背意愿之间的负向显著性关系。

此外，Myyry 等[69]还关注了个人价值观对遵从行为的影响作用，认为对变革持开放型态度的人将不会遵从信息系统安全政策。Son[35]的研究发现如果员工认为自己与组织的价值观一致（Perceived Value Congruence），那么他们愿意遵从信息系统安全政策。

4.2 政策相关的认知要素

感知合理性（Perceived Legitimacy）是员工对信息系统安全政策的适当性、满意性或者公平性的认知。信息系统安全政策是组织颁行的解释组织信息安全需求的正式文件，它明确界定了信息安全在实现组织目标中扮演的角色和支持作用[70, 71]。从员工的角度来讲，信息系统安全政策规定了员工在信息安全实践中的行为规范，即应该从事哪些行为和禁止从事哪些行为。员工对信息系统安全政策合理性的认识是员工遵从信息系统安全政策的重要前提[35, 59]。此外，Bulgurcu 等[72]发现员工对信息安全政策的质量（清晰性、完备性和一致性）和公平性的认知同样会正向影响遵从行为的发生。

4.3 个性特质因素

个人特质被认为是个体长期稳定的个性特征。信息安全行为领域的研究认为个性特征能够用来预测员工行为。针对个人特质的探讨有如下两点研究目的：一是针对不同性格的人对信息安全行为的不同响应对员工进行区分。在具体的管理实践中，通过性格特质作为指示器，可以比较准确的区别出哪些员工是信息系统安全政策的实施者，而哪些员工则会倾向于违背信息系统安全政策，从而可以通过采取不同的激励措施来控制信息安全风险行为的发生。二是针对不同性格的人对信息安全认知的不同响应可以设计更为有效的信息安全培训机制。此外，现有的研究结论还可以对企业员工的入职选拔与岗位分配提供指导性借鉴意义。

Shropshire 等[73]基于大五人格特质理论发现具有宜人性（宽厚、利他、谦和等）和尽责性（周到、负责、自我约束等）特质的员工倾向于从事 IT 安全遵从行为。Warkentin 等[74]同样引入大五人格特质理论中的宜人性、尽责性和开放性（创造力、好奇、思辨等）三种人格特质，探讨不同性格特质的员工对组织威慑效果和信息安全遵从态度的作用机制，及对计算机安全遵从意愿的影响作用。此外，Boss 等[45]发现即便是在组织强制的环境下，性格冷漠的人（Apathy）也不会主动采取信息安全预防措施。

控制观（Locus of Control）被经常用来探讨信息系统安全政策违背行为。控制观是个人对自己的行为方式和行为结果的责任的认识和定向，分内部控制观和外部控制观两种，前者指把责任归于个体的一些内在原因（如能力，努力程度等），后者则是指把责任或原因归于个体自身以外的因素（如环境因素，运气等）。Workman 等[75]发现持外部控制观的人比持内部控制观的员工更加不会遗漏实施安全预防措施。Chen 等[76]则证实外部控制观是预测员工互联网滥用行为的重要个性变量，持高外部控制观的员工更容易在工作中滥用互联网络。Ifinedo[55]证实了控制观与信息安全政策遵从行为之间的正向显著性关系。

5 文献整合与未来研究方向

综上，从“需求与控制”视角和“自我管理”视角对信息系统安全政策遵从和违背行为研究的关键要素进行归纳，构建理解员工从事信息系统安全政策遵从行为意愿和违背行为意愿的研究框架，如图 2 所示。

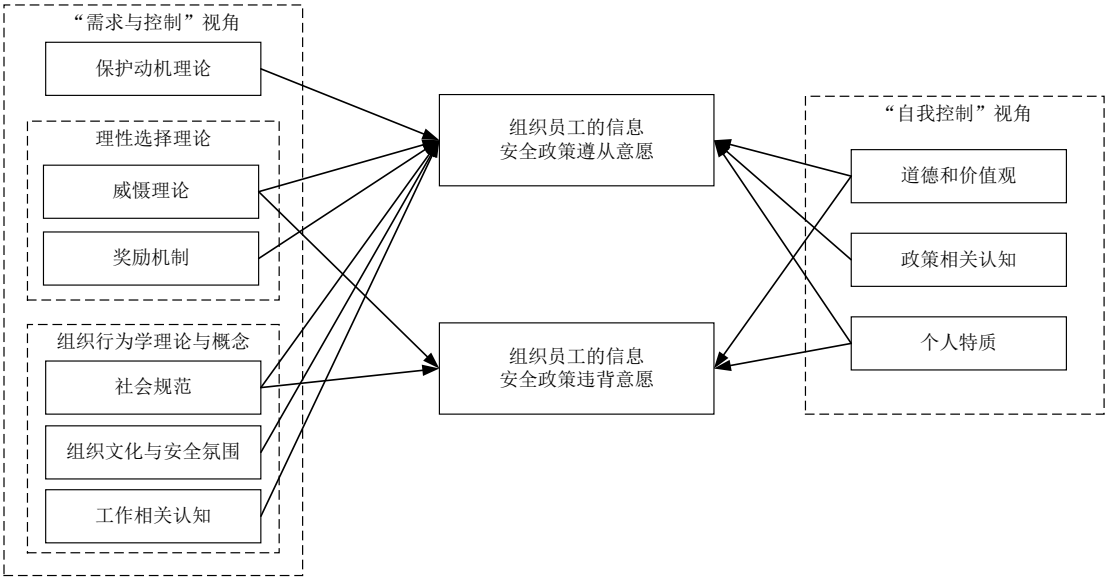

图 2 组织员工信息系统安全政策遵从与违背行为研究的理论框架

组织的信息安全除了必备的技术手段支持外，还依赖于组织内部对于信息系统安全政策的遵从和对违规行为的矫正。针对组织情境下员工的信息系统安全行为研究，国外研究大量引用犯罪学、社会学、组织行为学、心理学、健康学领域的理论就影响组织员工遵从和违背信息系统安全政策行为意愿的关键要素进行了实证探讨。针对国内信息安全研究倚重于技术层面和法律视角的研究现状，引入行为学观点，从“需求与控制”视角和“自我管理”视角对现有国内外文献进行了综述。本文归纳和分类了已有文献中涉及的主要信息安全行为，构建了组织员工信息系统安全政策遵从与违背行为的研究理论框架，针对已有研究中的结论差异进行总结，并揭示和解释研究结论产生差异的原因，是对国内信息安全行为研究的有益探索。针对组织情境下的信息系统安全行为研究还可以从如下几个视角进一步展开。

5.1 基于中国情境的信息安全行为研究和跨文化研究

国内信息安全领域的研究过度倚重于法律层面和技术方案，忽视了组织员工作为组织信息资产和信息技术的实际使用者的关键作用，员工的信息安全行为将直接影响组织的信息资产安全。此外，现有的研究理论是基于西方文化情境下的犯罪学、心理学、社会学、健康学等领域的借鉴，这些理论在中国文化情境下的适用性有待检验。而中国文化情境下的组织环境也有其新的特征，Hu 等[61]认为文化通过塑造人的价值观和加强组织承诺对员工的行为起作用，然而上述关系尚未被探讨。如受儒家文化的影响，员工往往会形成一种中庸保守的工作价值观，即过分的追求与周围同事的行为保持一致，而不是完全基于信息系统安全政策做出正确的行为取向判断，这有可能会使组织威慑的效果折扣；再比如中国文化中的人情关系也可能会削弱组织威胁的实际效果。因此，有必要在借鉴国内外现有研究成果的基础上形成并完善中国情境下的相关研究，构建基于中国文化情境的组织员工遵从信息系统安全政策行为的理论体系。

跨文化情境的比较研究同样重要。一方面，不同文化情境下研究结论的差异有助于理解文化差异对于信息系统安全政策遵从行为的作用机理，完善中国文化情境下的研究结论与理论构建；另一方面，跨文化研究对于借鉴国内外优秀的组织控制机制等管理方式到国内实践有着积极的现实意义。

5.2 组织控制机制的再探讨

国内外研究强调组织威慑与奖励激励的作用，然而两者在理论上和实践中发挥的作用存在争议。如何设计有效的组织正式控制机制是下一步研究需要重点思考的问题。如Wenzel[77, 78]发现社会规范在威慑与纳税遵从行为中起调节作用，而这种关系在信息安全行为研究中尚未被证实。现有针对个性特质的研究一般将个性特质作为信息系统安全政策遵从行为的直接前因变量。然而，个性特质作为调节变量的探讨早已开展[79]并应用于信息系统领域的探讨，有关于个性特质在组织控制机制中的调节作用的探讨将有助于了解不同个性特质的员工对于组织控制机制的认知差异，但是这种调节作用尚未在信息安全行为研究得到证实。

此外，已有研究在探讨组织非正式控制机制时往往默认同事间的相互影响和组织氛围是符合组织利益的积极行为，然而有关于组织行为学研究的相关结论表明，组织中存在一些不良习惯。如小团体中使用弱密码的行为有可能会演变为该群组成员的共性行为，由此导致组织威慑的形同虚设，是组织信息资产的潜在隐患。有关于组织非正式控制机制的引导和建设也应该在未来的研究中予以关注。

5.3 基于员工情绪视角的研究

信息系统安全政策在组织中的颁行往往带有自上而下的强制性，而员工却往往仅关注于自身值得去做的工作而不想付出额外的努力[29]，由此导致员工对于 IT 的使用不能完全遵从于组织意志，存在着诱发员工情绪偏离的潜在风险。Moody 等[80]证实情绪对员工在工作期间从事非工作相关的上网行为起到正向影响作用。Lwan[81]探讨了密码使用中的情绪响应对安全行为的关键性作用。早在 2008 年德勒发布的《第六次全球安全年度调查》中就已经开始关注情绪对于信息安全的影响作用，认为员工的心情或情绪原因导致的违规操作可能会成为信息安全遭受破坏的根源。翁勇南[19]通过案例分析构建组织内部威胁因素模型，认为情绪是信息安全中内部威胁者的动机之一。负向情绪是导致犯罪的重要原因[82]，而组织惩罚有可能会导致员工产生诸如焦虑不满等负向情绪，从而导致对信息安全制度和组织控制机制的敌对态度[40]。对员工情绪的探讨，有助于组织信息系统安全政策设计的合理性和人性化，以及信息安全意识培训体系的完善，然而，现有研究多基于员工的认知视角，尽管 Johnston 等[56]、Vance[52]和 Ifinedo[50]的研究基于恐惧诉求理论（Fear Appeal Theory）进行了探讨，但相关视角依然是侧重于从威胁认知和效用认知层面，没有对恐惧等负向情绪的作用进行直接探讨。有关于员工情绪与信息系统安全政策遵从和违背行为的探讨有待于进一步展开。

5.4 脑波成像方法在信息安全行为决策中的应用

当前的信息安全行为学研究方法主要是采用基于自陈式问卷调查（Self-reported）的统计实证方法。当然，为了获取员工对违规行为的态度和意愿，基于情境设计（Scenario Design）的问卷调查法被广为采用。然而，这类方法有着固有的缺陷，比如难以真实的捕捉实际行为和情绪响应过程。由此，这种方法上的局限性可能成为当前信息安全行为研究中惯常的以行为意愿作为结果变量，以及限制开展情绪视角下的信息安全行为研究的关键性原因。Hu 等[83]和 Vance 等[84]尝试将脑波成像方法引入信息安全行为学领域，借助脑波图像精准的度量员工在信息安全行为决策中的认知响应过程和决策过程。未来研究中可以通过跨学科合作，尝试该方法在信息安全行为决策研究中的更多可能性。

5.5 信息安全行为研究主题的细化

信息安全行为研究不应仅仅局限于对信息安全政策的相关行为决策的探讨，比如国外

诸多学者关注了信息安全培训[85, 86]和安全知识共享[87, 88]对员工行为的引导作用，越来越多的学者认为基于需要和控制视角的信息安全控制机制所对员工行为的限制效果远不如通过自我管理的方式所激发的自我主动性行为。而通过培训和知识分享等主题的探讨将有助于理解强化员工自我管理的方式与路径。此外，Yoon 等[89]关注了学生群体的信息安全行为，Li 等[90]和 Anderson 等[91]号召开展对家庭用户的信息安全行为进行研究。对研究群体的扩展可以更好的了解员工信息安全行为决策的产生，因为学生时期以及家庭用户的信息资产使用习惯等因素有可能会随着员工身份的转换而影响工作期间的信息安全行为。未来研究可以更加深入的对信息安全行为主体和研究对象进行细分，从行为学视角构建更为全面的信息安全行为研究体系。

参考文献

[1] Melville N, Kraemer K, Gurbaxani V. Review: Information technology and organizational performance: An integrative model of IT business value [J]. MIS Quarterly, 2004, 28(2): 283-322.

[2] PWC BIS Cyber Security Breaches Survey [EB/OL]. https://dm.pwc.com/HMG2013BreachesSurvey/,2014.

[3] Colwill C. Human factors in information security: The insider threat–Who can you trust these days? [J]. Information Security Technical Report, 2009, 14(4): 186-96.

[4] Herath T, Rao HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness [J]. Decision Support Systems, 2009, 47(2): 154-165.

[5] Information security breaches survey 2013: technical report [EB/OL].

https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report, 2013.

[6] Padayachee K. Taxonomy of compliant information security behavior [J]. Computers & Security, 2012, 31(5): 673-680.

[7] Crossler R E, Johnston A C, Lowry P B, et al. Future directions for behavioral information security research [J]. Computers & Security, 2013, 32: 90-101.

[8] Straub D W, Welke R J. Coping with systems risk: security planning models for management decision making [J]. MIS Quarterly, 1998, 22(4): 441-469.

[9] Siponen M T. On the role of human morality in Information System Security [M]// DHILLON G. Information Security for Global Information Infrastructures. United States of America; Idea Group Publishing. 2000: 401-410.

[10] Whitman M E. Enemy at the gate: Threats to information security [J]. Communications of the ACM, 2003, 46(8): 91-5.

[11] Guo K H. Security-related behavior in using information systems in the workplace: A review and synthesis [J]. Computers & Security, 2013, 32: 242-251.

[12] Willison R, Warkentin M. Beyond deterrence: An expanded view of employee computer abuse [J]. MIS Quarterly, 2013, 37(1): 1-20.

[13] 谷田. 网络环境下的企业信息安全问题研究 [D]. 郑州:郑州大学, 2012.

[14] 黄鼎隆. 信息安全感知模型及其应用 [D]. 北京: 清华大学, 2008.

[15] 王军. 信息安全的经济学分析及管理策略研究 [D]. 哈尔滨:哈尔滨工业大学, 2007.

[16] 王巧玲. 企业信息安全的组织因素及管理模型研究 [D]. 衡阳: 南华大学, 2012.

[17] 曾忠平. 信息安全人因风险研究进展综述 [J]. 情报杂志, 2014, 33(4): 6-11.

[18] 曾忠平, 杨哲, 刘春梅. 用户信息安全行为研究评述 [J]. 情报杂志, 2014, 33(12): 184-188.

[19] 翁勇南. 信息安全中内部威胁者行为倾向研究 [D]. 北京:北京交通大学, 2006.

[20] 常建轩. 企业信息安全策略成功实施的影响因素研究 [D]. 杭州:浙江大学, 2007.

[21] 李瀛. 员工信息安全违规意愿的实证研究 [D]. 大连: 大连理工大学, 2011.

[22] 陈琳. 影响员工遵从信息安全政策的要素研究 [D]. 大连: 大连理工大学, 2011.

[23] 李科. 影响员工互联网使用不当行为的因素分析 [D]. 杭州: 浙江理工大学, 2012.

[24] 石栩楠. 企业信息系统安全中员工行为的影响因素研究 [D]. 重庆:重庆大学, 2012.

[25] 程丽娇. 员工互联网滥用意愿影响因素的实证研究 [D]. 大连: 大连理工大学, 2013.

[26] 袁园园. 影响员工遵从互联网使用策略意向的因素分析--基于理性选择理论 [D]. 杭州: 浙江理工大学, 2012.

[27] 王冬梅. 理性选择视角下信息安全违背行为影响因素实证研究 [D]. 镇江: 江苏科技大学, 2014.

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

[29] Xue Y, Liang H, Wu L. Punishment, justice, and compliance in mandatory IT settings [J]. Information Systems Research, 2011, 22(2): 400-414.

[30] Siponen M, Vance A. Neutralization: New insights into the problem of employee systems security policy violations [J]. MIS Quarterly, 2010, 34(3): 487-502.

[31] Vance A, Siponen M T. IS security policy violations: a rational choice perspective [J]. Journal of Organizational and End User Computing, 2012, 24(1): 21-41.

[32] Hovav A, D'Arcy J. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea [J]. Information & Management, 2012, 49(2): 99-110.

[33] Guo K H, Yuan Y. The effects of multilevel sanctions on information security violations: A mediating model [J]. Information & Management, 2012, 49(6): 320-326.

[34] Herath T, Rao H R. Protection motivation and deterrence: A framework for security policy compliance in organisations [J]. European Journal of Information Systems, 2009, 18(2): 106-125.

[35] Son J-Y. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies [J]. Information & Management, 2011, 48(7): 296-302.

[36] Lee S M, Lee S-G, Yoo S. An integrative model of computer abuse based on social control and general deterrence theories [J]. Information & Management, 2004, 41(6): 707-718.

[37] D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach [J]. Information Systems Research, 2009, 20(1): 79-98.

[38] Li H, Zhang J, Sarathy R. Understanding compliance with internet use policy from the perspective of rational choice theory [J]. Decision Support Systems, 2010, 48(4): 635-645.

[39] Hu Q, Xu Z, Dinev T, et al. Does deterrence work in reducing information security policy abuse by employees? [J]. Communications of the ACM, 2011, 54(6): 54-60.

[40] Chen Y, Ramamurthy K, Wen K-W. Organizations' Information Security Policy Compliance: Stick or Carrot Approach? [J]. Journal of Management Information Systems, 2012, 29(3): 157-188.

[41] Liang H, Xue Y, Wu L. Ensuring Employees' IT Compliance: Carrot or Stick? [J]. Information Systems Research, 2013, 24(2): 279-294.

[42] Cheng L, Li W, Zhai Q, et al. Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory [J]. Computers in Human Behavior, 2014, 38: 220-228.

[43] Li H, Sarathy R, Zhang J. Understanding compliance with internet use policy: An integrative model based on command-and-control and self-regulatory approaches[C]. The proceedings of the International Conference on Information Systems, 2010.

[44] Guo K H, Yuan Y, Archer N P, et al. Understanding nonmalicious security violations in the workplace: a composite behavior model [J]. Journal of Management Information Systems, 2011, 28(2): 203-236.

[45] Boss S R, Kirsch L J, Angermeier I, et al. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security [J]. European Journal of Information Systems, 2009, 18(2): 151-164.

[46] Frederickson J R, Waller W. Carrot or stick? Contract frame and use of decision‐Influencing information in a principal‐agent setting [J]. Journal of Accounting Research, 2005, 43(5): 709-733.

[47] Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness [J]. MIS Quarterly, 2010, 34(3): 523-548.

[48] Ng B Y, Kankanhalli A, Xu Y C. Studying users' computer security behavior: A health belief perspective [J]. Decision Support Systems, 2009, 46(4): 815-825.

[49] Robert W Rogers. Cognitive and Physiological Processes in Fear Based Attitude Change: A revised Theory of Protection Motivation [M]. New York: Guilford Press. 1983.

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

[51] Siponen M, Adam Mahmood M, Pahnila S. Employees' adherence to information security policies: An exploratory field study [J]. Information & Management, 2014, 51(2): 217-224.

[52] Vance A, Siponen M, Pahnila S. Motivating IS security compliance: Insights from habit and protection motivation theory [J]. Information & Management, 2012, 49(3-4): 190-198.

[53] Rhee H S, Kim C, Ryu Y U. Self-efficacy in information security: Its influence on end users' information security practice behavior [J]. Computers & Security, 2009, 28(8): 816-826.

[54] Warkentin M, Johnston A C, Shropshire J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention [J]. European Journal of Information Systems, 2011, 20(3): 267-284.

[55] Ifinedo P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition [J]. Information & Management, 2014, 51(1): 69-79.

[56] Johnston A C, Warkentin M. Fear appeals and information security behaviors: An empirical study [J]. MIS Quarterly, 2010, 34(3): 549-566.

[57] Bobek D D, Hageman A M, Kelliher C F. Analyzing the role of social norms in tax compliance behavior [J]. Journal of Business Ethics, 2013, 115(3): 451-468.

[58] Merhi M I, Midha V. The impact of training and social norms on information security compliance: A pilot study. The proceedings of the 33rd International Conference on Information Systems[C], Orlando, 2012.

[59] Zhang J, Reithel B J, Li H. Impact of perceived technical protection on security behaviors [J]. Information Management & Computer Security, 2009, 17(4): 330-340.

[60] Todd Michael Dugo. The insider threat of organizational information security: A structural model and empirical test [D]. Auburn University, 2007.

[61] Hu Q, Dinev T, Hart P, et al. Managing employee compliance with information security policies: The critical role of top management and organizational culture [J]. Decision Sciences, 2012, 43(4): 615-660.

[62] Chang S E, Lin C S. Exploring organizational culture for information security management [J]. Industrial Management & Data Systems, 2007, 107(3): 438-458.

[63] D'Arcy J, Greene G. Security culture and the employment relationship as drivers of employees' security compliance [J]. Information Management & Computer Security, 2014, 22(5): 474-489.

[64] Chan M, Woon I, Kankanhalli A. Perceptions of information security in the workplace: Linking information security climate to compliant behavior [J]. Journal of Information Privacy & Security, 2005, 1(3): 18-41.

[65] Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: An action research study [J]. MIS Quarterly, 2010, 34(4): 757-778.

[66] Chang A, Wu C Y, Liu H W. The effects of job satisfaction and organization commitment on information security policy adoption and compliance[C]. The IEEE Proceedings of the Management of Innovation and Technology, 2012.

[67] Goo J, Yim M S, Kim D. A Path to successful management of employee security compliance: An empirical

study of information security climate [J]. IEEE Transactions on Professional Communication, 2014, 57(4): 286-308.

[68] Siponen M T. A conceptual foundation for organizational information security awareness [J]. Information Management & Computer Security, 2000, 8(1): 31-41.

[69] Myyry L, Siponen M, Pahnila S, et al. What levels of moral reasoning and values explain adherence to information security rules? An empirical study [J]. European Journal of Information Systems, 2009, 18: 126-139.

[70] Höne K, Eloff J. What makes an effective information security policy? [J]. Network Security, 2002, 2002(6): 14-16.

[71] Höne K, Eloff J. Information security policy - What do international information security standards say? [J]. Computers & Security, 2002, 21(5): 402-409.

[72] Bulgurcu B, Cavusoglu H, Benbasat I. Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: an empirical investigation[C]. The 43rd Hawaii International Conference on System Sciences, 2010.

[73] Shropshire J, Warkentin M, Johnston A, et al. Personality and IT security: An application of the five-factor model [C]. The Proceedings of the Americas Conference on Information Systems, 2006.

[74] Warkentin M, Carter L, McBride M E. Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies[C]. The Proceedings of the IFIP Workshop, 2011.

[75] Workman M, Bommer W H, Straub D. Security lapses and the omission of information security measures: A threat control model and empirical test [J]. Computers in Human Behavior, 2008, 24(6): 2799-2816.

[76] Chen J V, Ross W H, Yang H H. Personality and motivational factors predicting internet abuse at work [J]. Cyberpsychology, 2011, 5(1): 1-11.

[77] Wenzel M. The social side of sanctions: personal and social norms as moderators of deterrence [J]. Law and Human Behavior, 2004, 28(5): 547-567.

[78] Wenzel M. Motivation or rationalisation? Causal relations between ethics, norms and tax compliance [J]. Journal of Economic Psychology, 2005, 26(4): 491-508.

[79] Chaplin W F. The next generation of moderator research in personality psychology [J]. Journal of Personality, 1991, 59(2): 143-78.

[80] Moody G D, Siponen M. Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work [J]. Information & Management, 2013, 50(6): 322-335.

[81] Gulenko I. Improving passwords: Influence of emotions on security behaviour [J]. Information Management & Computer Security, 2014, 22(2): 167-178.

[82] Agnew R. Foundation for a general strain theory of crime and delinquency [J]. Criminology, 1992, 30(1): 47-88.

[83] Hu Q, West R, Smarandescu L, et al. Why Individuals Commit Information Security Violations: Neural Correlates of Decision Processes and Self-Control[C]. The 47th Hawaii International Conference on System Sciences, 2014.

[84] Vance A, Anderson B B, Kirwan B, et al. Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG) [J]. Journal of the Association for Information Systems, 2014, 15(10): 679-722

[85] Karjalainen M, Siponen M. Toward a new meta-theory for designing information systems (IS) security training approaches [J]. Journal of the Association for Information Systems, 2011, 12(8): 518-555.

[86] Waly N, Tassabehji R, Kamala M, et al. Improving Organisational Information Security Management: The Impact of Training and Awareness [M]. 2012.

[87] Hassan N H, Ismail Z. Investigation of key resistance factors in knowledge sharing towards information security culture in healthcare organization[C]. The 8th International Conference on Knowledge Management in Organizations, 2014.

[88] Hagen J M, Albrechtsen E. Effects on employees' information security abilities by e-learning [J]. Information Management & Computer Security, 2009, 17(5): 388-407.

[89] Yoon C, Hwang J W, Kim R. Exploring factors that influence students' behaviors in information security [J]. Journal of Information Systems Education, 2012, 23(4): 407-415.

[90] Li Y, Siponen M. A call for research on home users' information security behaviour [C]. the 15th Pacific Asia Conference on Information Systems, 2011.

[91] Anderson C L, Agarwal R. Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions [J]. MIS Quarterly, 2010, 34(3): 613-643.

Review of the Researches on Organization Employee's Information System Security Behavior

CHEN Hao, LI Wenli, KE Yulong

(Faculty of Management and Economics, Dalian University of Technology, Dalian,116023, China)

Abstract Employee's information security behavior is the important prerequisite to ensure the safety of organizational information assets. The existing researches of organizational information security are fragmented and not systematic, especially lack of studies from behavioral perspectives. The aim of this paper is to address this inadequacy by contributing to a fuller picture. We do an exhaustive literature study on theories and try to make sense of the conclusion differences, based on the "command-and-control" approach and "self-regulatory" approach, we comb the key factors affecting employee's information system security policy compliance and violation behaviors, then an integrative framework is developed to illustrate the relationships among these factors. In the end, recommendations for the future research are discussed.

Key words Information Security, Information System Security Policy, Compliance Behavior, Violation Behavior, Information Security behavioral Management

作者简介

陈昊（1986- ），男，山东泰安人，大连理工大学管理与经济学部，博士研究生，研究方向：信息安全行为管理；E-mail: ch9569@mail.dlut.edu.cn

李文立（1969- ），男，河南平顶山人,大连理工大学管理与经济学部副部长，博士生导师，研究方向:信息系统与信息行为,新兴电子商务理论与技术,复杂系统分析与管理；E-mail：wlli@dlut.edu.cn

柯育龙（1981- ），男，湖北大冶人，大连理工大学管理与经济学部，博士研究生，研究方向：信息安全行为管理；E-Mail：keyulong@mail.dlut.edu.cn