大连理工大学
管理论丛

企业员工的信息安全行为研究

李文立　陈　昊/著

科学出版社

大连理工大学管理论丛

企业员工的信息安全行为研究

李文立　陈　昊　著

国家自然科学基金项目（71272092，71431002，71731003）
国家自然科学基金创新研究群体项目（71421001）　　资助
大连理工大学基本科研业务费项目（DUT18RW129）

科学出版社

北　京

内 容 简 介

行为安全是组织信息安全管理体系不可或缺的组成部分。员工对于信息资产的合规使用是维护组织信息安全的关键环节，若员工有违规行为则会对信息安全带来潜在风险甚至巨大损失。本书以员工为基本研究单位，从行为学的角度探讨企业的信息安全管理，旨在揭示组织信息安全管理中员工的信息安全行为模式及形成与治理机制，从而为更好地制定和实施信息安全管理战略，建立和维持信息资产安全提供理论依据与实践指导。本书首先对组织信息安全管理，特别是行为安全管理的产生和研究现状进行回顾；其次从多理论视角，针对遵守信息系统安全政策的行为、违背信息系统安全政策的行为，以及互联网滥用行为进行深入探讨，揭示行为成因并提出相应的行为激励或治理对策。

本书可供信息安全管理研究方向高年级的硕士生、博士生及教师参阅；同时也可供企事业单位和政府部门相关管理工作者阅读。

图书在版编目（CIP）数据

企业员工的信息安全行为研究/李文立，陈昊著. —北京：科学出版社，2018.10

（大连理工大学管理论丛）

ISBN 978-7-03-058156-3

Ⅰ. ①企… Ⅱ. ①李… ②陈… Ⅲ. ①企业管理—信息安全—研究 Ⅳ. ①F272.7

中国版本图书馆 CIP 数据核字（2018）第 139193 号

责任编辑：李 莉 / 责任校对：李 影

责任印制：霍 兵 / 封面设计：无极书装

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京通州皇家印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2018 年 10 月第 一 版 开本：720×1000 1/16

2018 年 10 月第一次印刷 印张：10

字数：210000

定价：86.00 元

（如有印装质量问题，我社负责调换）

作者简介

李文立

大连理工大学管理与经济学部副部长、教授、博士生导师，教育部新世纪人才计划获得者，辽宁省教育厅电子商务类教学指导委员会主任委员，国际信息系统协会中国分会（China Association for Information Systems，CNAIS）理事，中国系统工程学会青年工作委员会常务理事，国家创新群体、教育部创新团队及国家重点学科“管理科学与工程”核心团队成员，大连理工大学电子商务中心副主任，大连市电子商务重点实验室副主任。主持国家自然科学基金重点项目 1 项、面上项目 5 项，在国内外重要学术期刊和国际会议上发表论文百余篇。主要研究领域为信息管理、电子商务。

陈昊

大连理工大学管理与经济学部博士研究生，加拿大麦克马斯特大学 DeGroote 商学院访问博士生。目前从事信息系统与信息安全管理，IT 安全与电子商务应用等方面的研究。研究成果发表在《管理科学》《科研管理》《管理评论》等国内信息系统 A 类期刊，PACIS（Pacific Asia Conference on Information Systems，即亚太信息系统会议）等重要国际会议，以及 *Information Technology & People* 和 *Behaviour & Information Technology* 等 SSCI 和 SCI 期刊。

丛书编委会

总　序

编写一批能够反映大连理工大学管理学科科学研究成果的专著，是几年前的事情了。这是因为大连理工大学作为国内最早开展现代管理教育的高校，早在1980年就在国内率先开展了引进西方现代管理教育的工作，被学界誉为“中国现代管理教育的先驱，中国MBA教育的发祥地，中国管理案例教学法的先锋”。大连理工大学管理教育不仅在人才培养方面取得了丰硕的成果，在科学研究方面同样取得了令同行瞩目的成绩。例如，2010年时的管理学院，获得的科研经费达到2 000万元的水平，获得的国家级项目达到20多项，发表在国家自然科学基金委员会管理科学部的论文达到200篇以上，还有两位数的国际SCI、SSCI论文发表，在国内高校中处于领先地位。在教育部第二轮学科评估中，大连理工大学的管理科学与工程一级学科获得全国第三名的成绩；在教育部第三轮学科评估中，大连理工大学的工商管理一级学科获得全国第八名的成绩。但是，一个非常奇怪的现象是，2000年之前的管理学院公开出版的专著很少，几年下来却只有屈指可数的几部，不仅与兄弟院校距离明显，而且与自身的实力明显不符。

是什么原因导致这一现象的发生呢？在更多的管理学家看来，论文才是科学研究成果最直接、最有显示度的工作，而且论文时效性更强、含金量也更高，因此出现了不重视专著也不重视获奖的现象。无疑，论文是重要的科学研究成果的载体，甚至是最主要的载体，但是，管理作为自然科学与社会科学的交叉成果，其成果的载体存在方式一定会呈现出多元化的特点，其自然科学部分更多的会以论文等成果形态出现，而社会科学部分则既可以以论文的形态呈现，也可以以专著、获奖、咨政建议等形态出现，并且同样会呈现出生机和活力。

2010年，大连理工大学决定组建管理与经济学部，将原管理学院、经济系合并。重组后的管理与经济学部以学科群的方式组建下属单位，设立了管理科学与工程学院、工商管理学院、经济学院以及MBA/EMBA教育中心。重组后的管理与经济学部的自然科学与社会科学交叉的属性更加明显，全面体现学部研究成果

的重要载体形式——专著的出版变得必要和紧迫了。本套论丛就是在这个背景下产生的。

本套论丛的出版主要考虑了以下几个因素：第一是先进性。要将学部教师的最新科学研究成果反映在专著中，目的是更好地传播教师最新的科学研究成果，为推进管理与经济学科的学术繁荣作贡献。第二是广泛性。管理与经济学部下设的实体科研机构有 12 个，分布在与国际主流接轨的各个领域，所以专著的选题具有广泛性。第三是纳入学术成果考评之中。我们认为，既然学术专著是科研成果的展示，本身就具有很强的学术性，属于科学研究成果，有必要将其纳入科学研究成果的考评之中，而这本身也必然会调动广大教师的积极性。第四是选题的自由探索性。我们认为，管理与经济学科在中国得到了迅速的发展，各种具有中国情境的理论与现实问题众多，可以研究和解决的现实问题也非常多，在这个方面，重要的是发动科学家按照自由探索的精神，自己寻找选题，自己开展科学研究并进而形成科学研究的成果，这样的一种机制一定会使得广大教师遵循科学探索精神，撰写出一批对于推动中国经济社会发展起到积极促进作用的专著。

本套论丛的出版得到了科学出版社的大力支持和帮助。马跃社长作为论丛的负责人，在选题的确定和出版发行等方面给予了自始至终的关心，帮助学部解决出版过程中的困难和问题。特别感谢学部的同行在论丛出版过程中表现出的极大热情，没有大家的支持，这套论丛的出版不可能如此顺利。

大连理工大学管理与经济学部

2014 年 3 月

前　言

信息安全事件的频发给企业造成巨大的经济损失和声誉损害。组织员工产生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。信息安全不单单需要安全技术的支撑和法律体系的完善，还需要从管理层面关注信息安全风险的人因要素。行为信息安全同样是企业信息安全管理的重要组成部分和关键环节。本书旨在揭示企业信息安全管理中员工的信息安全行为模式及形成与治理机制，从而为企业更好地制定和实施信息安全管理战略，建立和维护企业的信息资产安全提供理论依据与实践指导。

本书以企业员工为基本研究单位，从行为学的角度探讨企业的信息安全管理。企业实践中，员工需要在信息系统安全政策（information security policies，ISP）的规定范畴内实施角色内行为，以确保企业可以及时响应信息安全风险，从而使企业时刻处于安全氛围之中。员工遵守信息系统安全政策与否需要企业发挥控制约束力，以确保员工可以满足组织对于信息安全的期望而遵守信息系统安全政策的相关规定，并以此为信息资产使用过程中的行为准则，同时避免做出违背信息系统安全政策的举动。本书针对员工的信息系统安全政策遵守行为和信息系统安全政策违背行为，及其特例互联网滥用行为，从不同的理论视角，尝试探讨影响行为成因的关键要素及其影响机理。研究结论为企业的信息安全行为管理实践提供借鉴，通过组织信息安全伦理氛围建设、道德培训开展和控制机制（奖惩激励、面子管理、社会纽带和社会压力等）设计来约束和矫正员工的消极信息安全行为。

本书是大连理工大学管理与经济学部李文立教授 IT 行为研究团队集体智慧的结晶，得到国家自然科学基金项目（71272092，71431002，71731003），国家自然科学基金创新研究群体项目（71421001）和大连理工大学基本科研业务费项目（DUT18RW129）的支持资助。全书内容来源于李文立教授研究团队多年的研究成果，由李文立教授和博士研究生陈昊进行统筹和内容整理工作。全书内容安排如

下：第 1~3 章和第 5 章内容源自博士研究生陈昊的研究成果；第 4 章内容源自硕士研究生陈琳的研究内容；第 6 章和第 7 章参考了硕士研究生程丽娇和李瀛的研究工作。

由于时间和水平有限，书中难免存在不足之处，敬请读者不吝指正。

目　录

第 1 章　绪论……1
1.1　企业信息安全行为管理……1
1.2　研究范畴……3
1.3　研究内容……7
1.4　内容与结构安排……9
1.5　小结……11
参考文献……11
第 2 章　信息安全行为研究现状……15
2.1　信息安全……15
2.2　信息安全管理……16
2.3　信息安全行为研究……19
参考文献……27
第 3 章　组织控制与信息系统安全政策遵守行为：面子需求倾向的调节作用……33
3.1　问题描述……33
3.2　正式控制与奖惩激励……34
3.3　非正式控制与面子管理……36
3.4　研究模型……38
3.5　研究设计……41
3.6　数据处理与结果……44
3.7　研究贡献与管理启示……49
3.8　小结……50
参考文献……50
第 4 章　直接领导、结果期望与威慑对信息系统安全政策遵守意愿的作用研究……54
4.1　问题概述……54
4.2　社会认知理论……54

4.3 威慑理论……56
4.4 研究模型……57
4.5 研究设计……59
4.6 数据处理与结果……63
4.7 研究结论与不足……65
4.8 小结……66
参考文献……67
第 5 章 道德推脱与信息系统安全政策违背意愿的关系研究：以组织伦理氛围为调节变量……69
5.1 问题概述……69
5.2 道德推脱与违规行为……69
5.3 组织伦理氛围的调节机制……73
5.4 研究模型……76
5.5 研究设计……77
5.6 数据处理与结果……83
5.7 研究贡献与管理启示……89
5.8 小结……91
参考文献……91
第 6 章 社会纽带、社会压力与威慑对员工违背信息系统安全政策的影响研究……95
6.1 问题描述……95
6.2 社会控制机制……95
6.3 研究模型……98
6.4 研究设计……101
6.5 数据处理与结果……106
6.6 研究贡献与管理启示……109
6.7 小结……111
参考文献……112
第 7 章 基于中和技术和理性选择的互联网滥用行为意愿研究……114
7.1 问题描述……114
7.2 互联网滥用……114
7.3 理论基础与研究模型……118
7.4 研究设计……124
7.5 数据处理与结果……127
7.6 研究贡献与管理启示……136
7.7 小结……139
参考文献……140
后记……144

第1章 绪 论

1.1 企业信息安全行为管理

1.1.1 行为安全是组织信息安全管理体系不可或缺的组成部分

人们对信息安全的关注起始于20世纪中叶通信领域对信息加密传输的需求。在相当长的一段时期内，信息安全被等同于信息加密，其主要目的在于保障信息的机密、完整和可用。随着90年代互联网的兴起与普及，人们对于信息安全的认识已经不再局限于对数据信息本身的狭隘理解，而是逐渐将信息系统和互联网系统纳入其中，探求如何保障系统整体的安全性。随着信息技术和信息系统在商业组织中被广泛采纳，组织层面的信息安全面临着严峻的形势和挑战。特别是近年来大数据和“互联网+”概念的频繁提及与商业实践，使得信息资产的商业价值凸显，各类新兴互联网公司纷纷创立，越来越多的传统型企业也参与其中。然而，信息安全事件的频发对企业信息资产的安全使用提出了更为严峻的挑战，信息安全显得非常重要。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[1]，44%的中国内地及香港企业称遭遇过数据丢失或损坏事故，亚太地区的信息安全事件较上年增长21%[2]。2015年调查发现全球企业遭受的信息安全事件较2014年飙升38%[3]，超过45%的国内企业在过去三年内发生过不同量级的信息安全事故，大型企业（500人以上）与电信行业的信息安全事故发生比例分别高达57%和64%[4]。信息安全事件的频发和高发给企业造成巨额经济损失。在中国内地和香港，2013年因信息安全事件，企业平均经济损失高达180万美元，高于亚太地区的平均值160万美元[2]；2015年英国大型企业的损失则高达314万英镑[3]。

人们在信息安全问题的产生之初倾向于从技术角度寻求相应的解决方案，密码学、可信计算、网络安全和信息隐藏等技术的急速更新为信息设备安全、数据安全和内容安全提供了硬件和软件的底层安全保障[5]。商业组织的信息安全实践同样倚重于基于安全技术的解决方案，以防范信息安全事件的发生。引入信息安全技术架构、应用新技术工具和平台、安装防火墙及安全防护软件、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在一定程度上为信息资源提供安全保护[6, 7]。2015 年，44%的英国大型企业增加了信息安全投资预算，并且被调查企业中有近 1/3 选择投资于安全控制技术[8]。

安全技术的实施效果取决于员工对于安全技术的采纳与使用。员工不正确的使用习惯，对信息资产的滥用和误用行为等（如未经授权登录系统或访问数据、违背数据保护规范或章程、丢失或泄露机密信息等[8]）都无法通过技术手段来进行控制[9, 10]。并且员工在高效的安全技术支持和其他组织安全对策的支持下表现出松懈与疏忽[11~13]，从而丧失了对信息安全威胁应有的敏感性和快速响应。2013 年调查数据显示，英国 74%的信息安全事件与内部员工相关[14]；同年，国内调查数据表明，81%的企业信息安全泄密类问题发生在体系内部（内部人员过失泄密或主动窃密），由外部黑客攻击、系统漏洞、病毒感染等问题带来的信息泄密案例，仅有 12%；内部体系造成的泄密损失是黑客攻击的 16 倍，是病毒感染的 12 倍[15]。2015 年的调查数据发现内部人员导致的信息安全事件较 2014 年增加 22%[3]。信息安全问题已不仅仅是单纯的 IT 技术问题，更涉及组织对员工的行为管理层面。越来越多的研究人员和企业实践认同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[16]，行为安全同样是信息安全管理的重要组成部分。

1.1.2 对员工行为的约束与引导是实现行为安全的关键

企业高层推行信息系统安全政策及安全教育培训和意识项目（security education, training and awareness，SETA）来规范员工的信息安全行为的做法已被广泛应用于国外企业的信息安全实践。信息系统安全政策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[17]。2015 年数据显示，98%的英国大型企业和 60%的中小型企业都制定过信息系统安全政策文件[8]。安全教育培训和意识项目则致力于提高员工的信息安全意识和道德水平，并明确员工对于威慑严重性和确定性的认知[18]，从而提升用户遵守信息系统安全政策的意愿并确保安全解决方案的使用[19]。2015 年，英国企业用于员工培训的信息安全投资比例达到 26%[8]，针对员工开展安全意识培训的大型企业比例由 58%（2013 年）上升至 72%（2015 年）。然而，员工对信息系统安全政策的认可与遵守并没有达到组织期望的程度。2011 年调查数据显示，国内超过七成的员工承认他们在绝大多数的工作时间内不会遵守信息系统安全政策的规定，尽管 36%的员工意识到他们应该对信息安全负主要责任[20]。

遵守信息系统安全政策是保障企业信息资产安全的前提。挖掘影响员工遵守信息系统安全政策的关键要素，并揭示其作用机制，是当前企业行为安全管理的瓶颈问题，也是当前行为学视角下信息安全研究的重要课题。现有研究发现理性

选择[21]、中和技术[22, 23]、心理抗拒[24]、威慑[25]、低自我控制[26, 27]是员工违背信息系统安全政策的重要原因，同时也揭示了道德[28]、自我效能[29]、主观规范[30]等对于员工遵守信息系统安全政策的关键性作用。然而，当前研究大多是基于犯罪学、心理学、健康护理学等领域理论的探讨，这些理论被应用到信息安全行为学研究中或多或少会存在理论应用适配性的问题。另外，当前研究存在诸多不一致的研究结论，如基于威慑理论进行的探讨得出了互相矛盾的研究结论[31]。这些研究结论在一定程度上阻碍了信息安全实践，也为后续研究提供了空间。同时，组织中涉及员工行为的信息安全问题是组织行为学的研究范畴，然而组织行为学相关的理论较少地被应用于探讨信息安全行为。

1.1.3 信息安全战略的提出为中国行为安全研究提供新契机

近年来，信息安全上升为国家战略，国家出台了《工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见》等指导文件，并通过设立国家网络安全宣传周等活动，推动全社会对信息安全的重视，从国家政策和氛围层面为信息安全提供了强有力的导向支持。然而，中国内地及香港作为全球信息安全事件的高发区，客户资料泄露、员工身份盗用、数据损坏和丢失等信息安全问题的发生比例逐年递增，而这些信息安全事件的发生有37%源自员工的不当操作[2]。近年来诸如电信内部员工泄露用户隐私[1]等信息安全事件的频频发生，突显出企业在信息安全行为管理上的薄弱与乏力。尽管有七成受访企业认为信息安全应该引起高度重视，然而57%的安全从业者并未参加过相关的信息安全培训，平均接近三成的中小型企业尚未配备信息安全团队，并缺乏信息安全投入[4]。国内企业面临的信息安全形势非常严峻。

企业信息安全管理体系的构建，离不开安全技术的基本保障和制度流程的安全控制，还需要在信息资源的使用过程方面对员工进行规范和引导。国内对信息安全的研究过度集中于探讨技术层面的安全解决方案[32]，从行为学视角探讨如何约束和引导员工的信息安全实践是组织和学界当前亟须解决的难点问题。基于以上分析，将对中国情境下组织员工的信息安全行为影响要素进行探讨，是对信息安全行为研究的重要完善和补充，也是对本土化信息安全行为研究的有益探索。

1.2 研 究 范 畴

1.2.1 相关概念

信息安全领域出现了大量的专有名词。2005年制定的GB/T 19715《信息技术

信息技术安全管理指南》国家标准中使用“IT 安全”的概念，并将其定义为“与定义、获取和维护保密性、完整性、可用性、可核查性、真实性和可靠性有关的各个方面”。该概念的提出在具体内涵上存在细节性的差异，然而本质上与信息安全的概念是一致的。此外，在一些政策性文件中还出现了“网络安全”，如中央网络安全和信息化领导小组使用了“网络安全”的名称。尽管存在名称上的不一致，但是在实际的研究中，这些概念涵盖在信息安全的大范畴之内，研究中也不再进行细分。

另外，von Solms 和 van Niekerk[33]将赛博安全（cyber security，CS）与信息安全进行了对比，认为两者最关键的区别在于赛博安全更加关注信息交互过程中的人、社会或国家的利益，如网络欺凌（cyber bulling）、家庭自动化（home automation）、数字媒体（digital media）和网络恐怖主义（cyber terrorism），其中涉及了诸如非信息性资产（non-information based assets），如智能家居被入侵可能会造成人身或财产伤害，影视音乐等媒体资源的盗版传播等会造成正版用户的损失。赛博安全关注在信息和通信技术（information and communication technology，ICT）被广泛应用的情境下所带来的全新信息安全挑战，即 ICT 的采纳产生的非信息性资产受到威胁。林润辉等[34]在此基础上将信息系统看作一种重要的 ICT，探讨信息安全、信息系统安全和赛博安全之间的关系，如图 1.1 所示。

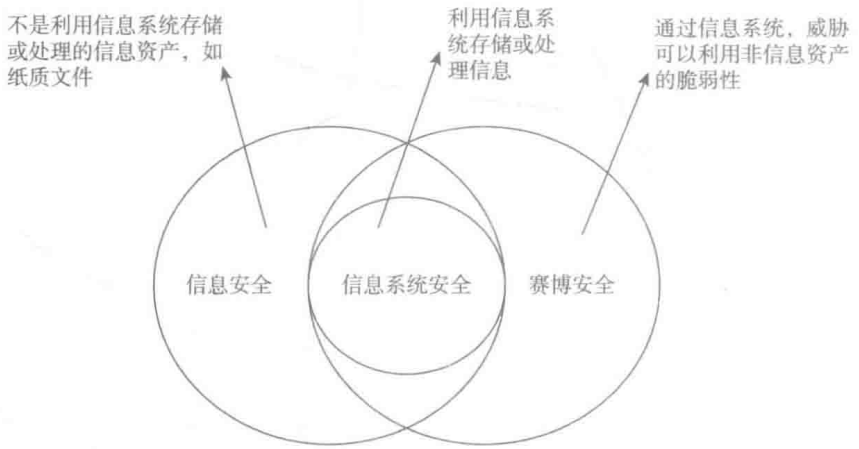

图 1.1 信息安全、信息系统安全和赛博安全的关系

本书对信息安全的探讨不涉及非信息资产。尽管 Cheng 等[35]在其研究中探讨了员工非授权阅读纸质机密文件的违规情境，但是现有研究更加关注信息系统相关的安全问题。据此，将重点探讨信息系统安全，即使用信息系统作为信息存储和处理介质，在对信息、信息系统及相关存储设备和应用程序等信息资产进行操作的过程中所产生的安全风险。

1.2.2 信息安全行为的分类

组织员工的信息安全行为（information security behaviors of employees，ISBE）是指组织中的员工在面对或使用组织中的信息资源（软硬件、数据、机密文件、资料等）时所采取的行为，如针对信息的保护性行为（安装防病毒软件）或破坏性行为（偷窃、泄密等）。信息安全行为领域的研究针对安全相关的行为并未形成统一的分类标准[36]，本书探讨两种类型的行为。

1. 信息系统安全政策遵守行为

信息系统安全政策遵守行为是指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信息资源的全部活动。例如，按照要求设置强密码、定期更新安全补丁、使用安全防护软件等。遵守信息系统安全政策的规定是保障企业信息资产安全的前提。探讨影响员工遵守信息系统安全政策的关键要素，并揭示其关键作用机制，是当前企业行为安全管理的瓶颈问题，也是当前行为学视角下信息安全研究的重要课题。本书的第 3 章和第 4 章针对信息系统安全政策遵守行为进行探讨。

2. 信息系统安全政策违背行为

信息系统安全政策违背行为是指员工忽视或违反信息系统安全政策的行为。该行为可能是员工的意识性行为或无意识行为，对信息资产安全带来实际损失或潜在性风险。已有研究中出现频率较高的五类消极信息安全行为，即计算机（或信息系统）滥用/误用（computer/IS misuse/abuse）、不道德的计算机使用（unethical computer using behavior）、非恶意安全违规行为（nonmalicious security violations）、互联网滥用/非工作相关的上网行为（internet abuse/non-work-related computing）和信息安全疏漏行为（information security omission behavior/knowing-doing gap）实质上都涉及对信息系统安全政策的违背，故统一归类为信息系统安全政策违背行为。五类消极信息安全行为的含义及示例如表 1.1 所示。

表 1.1 消极信息安全行为含义与示例

行为及类别	含义	示例
计算机（或信息系统）滥用/误用	员工非授权或故意滥用组织信息系统资源（如软硬件/数据和计算机服务等）的行为	使用盗版软件、非法访问数据、未经授权修改数据等
不道德的计算机使用	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
非恶意的安全违规行为	员工出于非主观恶意的目的实施违规行为	在便签上记录密码、设置简单密码等
互联网滥用/非工作相关的上网行为	员工在工作场所出于个人目的而使用互联网的行为	通过社交媒介聊天、浏览无关网页等

续表

行为及类别	含义	示例
信息安全疏漏行为	员工意识到信息安全风险但无视信息系统安全政策的行为	从未更换密码、不升级系统补丁、不进行备份数据等

注：根据文献[36]的研究整理和修改

组织行为学在探讨员工行为的时候不仅仅关注正面的积极行为，还关注消极的反生产行为或非伦理行为，以了解员工不合作或者不作为表现的背后动机与原因。消极的员工组织行为不仅违背组织的价值取向和规章制度，还可能会对企业绩效及声誉造成不同程度的损害，甚至为企业带来某些潜在的风险。类似地，信息系统安全政策遵守行为与信息系统安全政策违背行为不能简单地看作同一个问题的正、反两个方面。就现有的研究结论来看，解释遵守行为的要素往往不能够用于解释违背行为，有必要对这两种行为背后的形成机理分别做出各自的探讨。对信息系统安全政策遵守行为的探讨有助于了解员工对于信息安全的基本态度和认知，而对于信息系统安全政策违背行为的探讨则有助于反映当前组织信息安全管理中的疏漏与不足。两者相互补充，共同为企业的信息安全管理实践提供全面理解。第 5~7 章针对信息系统安全政策违背行为进行研究。

1.2.3 研究对象选择

本书针对企业中的员工开展信息安全行为学研究，研究中涉及的变量及其测度都是基于个体层面。研究对象定位于实行了信息系统安全政策的企业中的普通员工，而不仅仅局限于 IT 支持部门的特定员工或高层管理者。这是因为绝大多数的普通员工都涉及并参与信息资源的使用，是执行信息系统安全政策和履行信息安全义务的实施主体。他们对信息系统安全政策的违背将对组织带来不同程度的潜在风险或实质性危害。普通员工的信息安全行为能够在更广泛的层面上反映出企业信息安全管理中的潜在问题。

数据样本的采集对象同样选择普通员工。有学者认为在组织心理学和行为学研究中采用学生样本得到的研究结论和采用员工样本得到的结论并无本质性差别[37]。考虑到高校学生具有较强的信息系统或计算机使用技能和工作伦理意识，Lee 等[38]采用学生样本对互联网滥用行为进行了探讨。然而，现有的绝大多数信息安全行为学研究文献均采用具有实际工作经验的员工抽样样本，本书遵循大多数研究的采信方法。

1.2.4 研究行业选取

已有研究对于行业或者企业性质没有特别的区分。除去某些专注于特定行业