信息安全管理研究回顾、脉络梳理及未来展望*

林润辉[1],谢宗晓[1],刘琦[2]
(1.南开大学 商学院,天津 300071;
2.河南警察学院信息安全系,郑州 450002)

摘 要 信息安全随着信息化程度的提升受到了前所未有的关注。本文按照管理学的四个基本范式:功能范式、诠释范式、激进人本范式和激进结构范式对现有的信息安全管理研究进行了回顾,然后按照范式-时间以及范式-内容两种方法对主要研究进行了脉络梳理,最后总结了目前研究所存在的不足并给出了深入研究的方向。

关键词 信息安全,信息系统安全,管理学范式
中图分类号 C931.6

1 引言

随着"棱镜门"等事件的发生,信息安全受到前所未有的关注。但是,无论在研究领域还是实践中,一直存在着"重技术,轻管理"的错误认识,据《2010/2011 计算机犯罪与安全调查》(*Computer Crime and Security Survey*)报告:被试组织中杀毒软件和防火墙的使用率分别达到了97%和94.9%,但是49%的被试组织没有安全意识教育或没有相应的有效性测量机制,结果有41.1%的受访组织经历了信息安全事件。事实上,单纯通过技术手段获得的安全是有限的,缺乏相应的策略或流程的技术部署甚至是无效的[1-3],所以,获得信息安全不但需要技术手段(通过IT解决IT安全),还需关注策略和规程等管理手段(通过管理解决IT安全),甚至改变组织架构以适应不断变化的安全形式。

基于管理学视角的信息安全研究一直比较匮乏。虽然Dhillon和Backhouse[4]在2001年就对之前的研究进行了梳理,并得出结论:信息安全的研究方向必然转向社会科学视角。Siponen[5]则沿着信息安全的发展脉络将其分为五个阶段,并且认为第五阶段的信息安全方法将着眼于基于社会科学和可适应性的方法。这两篇综述文献为后续的研究指明了清晰的方向,但都存在如下不足:

(1)将"信息安全"(Information Security,IS)理解成更狭义的"信息系统安全"(Information System Security,ISS),导致对文献的述评都是从信息系统的研究领域开始,遗漏了一些重要的相关研究,尤其是起源于管理创新(Management Innovation)类的文献;

(2)没有严格区分"信息安全技术"(Information Security Technology,IST)和"信息安全管理"(Information Security Management,ISM),导致所讨论的信息系统安全包括了一部分技术,但是又不

* 基金项目:国家自然科学基金重点项目(71132001)。
通信作者:谢宗晓,南开大学商学院,博士研究生,E-mail:xiezongxiao@vip.163.com。
感谢Labovitz School of Business and Economics,University of Minnesota Duluth李大辉教授审阅全文并给出诸多建议。
感谢两位匿名审稿专家的修改意见,尤其是概念表达不清和研究框架引入突兀等意见,我们均重新做了表述。

全面，例如没有涉及密码学(Cryptography)等更主流的技术研究方向。

基于此，本文中：

(1) 只对信息安全管理领域的研究进行述评，不包括密码学、防火墙、防病毒和入侵检测系统(IDS)等信息安全技术；

(2) 对脉络的梳理，不局限于从信息系统研究到信息安全研究的常见路线，也包含了制度、社会、文化等如全面质量管理(Total Quality Management，TQM)等管理创新到信息安全管理的研究脉络分析。文中首先提出一个基于研究范式的概念框架用来将已有研究进行分类追踪，然后，第三部分到第六部分依照该概念框架对已有文献分别进行了述评，最后一部分按研究范式和时间前后两个维度进行了梳理，并给出了目前研究的不足和未来的研究方向。

2 概念及框架

2.1 相关概念

针对已有综述文献的不足之处，本文中首先区分“信息系统安全”和“信息安全”的概念，并限定“信息安全技术”与“信息安全管理”的范畴。

(1) ISO/IEC27002：2005 将信息安全定义为：保证信息的保密性、完整性和可用性；另外也可包括例如真实性、可核查性、不可否认性和可靠性等。在 ISO/IEC27000：2009 中特别强调“信息”是广义的概念，可能存在于各种介质，例如纸、计算机和人的大脑中等。显然，“信息系统安全”只是“信息安全”的一部分。

(2) 在实际应用中，“信息安全管理”和“信息安全技术”很难分开部署，例如：加解密算法是技术，而密钥管理则是安全策略。从研究起源而言却是可以区分的，例如：非对称密码算法主要以数学中的单向函数为基础，而防火墙和防病毒等与其他信息技术的研发也并无本质不同，追根溯源是技术与工程问题。但是信息安全制度的设计、员工安全策略遵守和用户参与对信息安全的影响等相关研究则起源于心理学、社会学和犯罪学等社会科学领域。在本文中所讨论的“信息安全管理”专指这些起源于社会科学的相关研究，换句话说就是更关注与“广义的信息”安全相关的人类行为。

2.2 框架安排

由于本文的目的不仅仅是回顾文献，更在于梳理其研究脉络，从而得到未来的研究方向，因此设计一个概念的框架是有必要的，Brrrell& 和 Morgan[6] 认为理清楚理论概念非常重要，这可以使研究者抛开研究的表面细节，而抓住隐藏于背后的理论基础。他坚信所有的组织理论都建立在科学哲学与社会理论基础之上，这也是其主要的两条轴线，关于科学本质的假设是从主观还是客观，关于社会(及组织等)本质假设则是有秩序的还是激变的。社会科学的客观维度往往被描述为“实证主义”(Positivism)，是将自然科学中的模型和方法应用到关于人的研究中。秩序强调社会(及组织等)的稳定性和连续性，而激变则强调社会冲突与统治。根据这两条轴线，抽象为四种范式，如图 1 所示。

功能范式认为社会是秩序的，科学的本质是客观的，作为研究者应该站在客观的角度去发现并试图支配规律，致力于解决实践中出现的信息安全问题，功能范式一度是早期信息安全领域研究的主

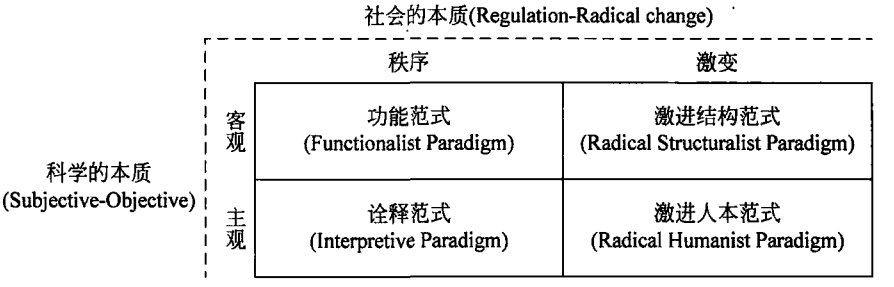

图1 由两个维度划分出的四种范式

流。虽然诠释范式也承认社会是秩序的，但从主观分析的角度去理解可以归结到社会环境而导致的个人或组织安全行为。激进人本范式认为社会是激变的，认为人的意识是由他所接触的意识形态上层建筑所控制，由此导致的“疏离感”或“错误意识”抑制了个人自我实现，并最终实现了一部分人对另一部分人的统治。激进人本范式对研究个体安全行为有很大的贡献[7]，激进结构范式和功能范式一样，也试图建立一种规范的理论体系和概念架构，但是认为组织及其管理充满着利益矛盾与斗争，因此常关注因制度原因而产生的管理问题。

这四种范式相互排斥，无论是其理论范式还是其方法论范式，都可以纳入 Brrrell& 和 Morgan[6] 的范式分类，且只能属于其中某一种[7]。目前在诸多研究领域，如运营管理、知识管理、信息系统开发和系统动态学等，当然也包括文献[4]，都据此进行了分类和梳理，信息安全管理作为管理学的一个分支，不是计算机科学和社会科学的简单结合，或各种社会科学理论的简单情境应用，而是产生于迥然不同的各种思想和研究方法相互之间复杂的缠绕。在信息安全管理研究领域，运用这四个范式理解信息安全方法的发展过程是重要也是相对合理的，可以使后续研究者从方法论或范式的角度理解现有的文献，从而使研究者忽略细枝末节，理清其理论起源并认清其哲学假设或前提[4]。

2.3 文献筛选与统计

在 EBSCO 和 ScienceDirect 数据库中限定“MIS Quarterly”、“Information Syetem Research”和“Journal of Management Information Systems”信息系统类影响因子排名前三位的最重要期刊，查阅标题中含“Information Security”“Information System Security”或标题中含“Risk Management/Assessment/Analysis”或“Weakness/Vulnerability/Threat”或“Computer Abuse”且摘要中含有“Information Security”，上述期刊中，共查阅到论文 49 篇。然后，将期刊限定为：“Administrative Science Quarterly”、“Academy of Management Journal”、“Academy of Management Review”以及“Management Science”几个管理类重要期刊，没有与信息安全相关的文献。将上述文献逐篇筛选，选择标准为有理论基础的实证研究，确定论文 19 篇。最后将期刊范围扩大至“Journal of the Association for Information Systems”、“Communication of the ACM”、“Information & Management”、“Decision Sciences”和“Decision Support Systems”信息系统类比较重要的期刊，将相关论文按照上述标准加论文引用次数筛选，确定论文 6 篇。

在 CKNI 中查询研究主题为“信息安全管理”或“信息系统安全管理”，且期刊级别限定为 CSSCI，共 77 篇，但满足“有理论基础的实证研究”条件的只有 1 篇。统计结果如表 1 所示。

表 1 筛选论文的统计结果

期刊名称(筛选出的论文数)	备 注
Administrative Science Quarterly(0) Academy of Management Journal(0) Academy of Management Review(0) Management Science(0) Strategic Management Journal(0)	这些期刊中关于信息安全甚至关于信息系统的论文都非常少,但关于管理创新的研究比较丰富。有些信息安全管理研究关注 ISMS① 和 SOX② 等管理创新接受,例如:文献[13]。Management Science 有 2 篇关于信息安全产业的和 1 篇补丁管理的,但不符合筛选条件
MIS Quarterly(13) Information System Research(5) Journal of Management Information Systems(1)	MIS Quarterly 2010. 34(3)为信息安全专刊,因此论文较多。该期刊自 1990 年至今一直关注计算机滥用(Computer Abuse)等信息安全问题,例如:文献[8]以及文献[30]都是关于该选题的,Detmar W. Straub 目前为 MIS Quarterly 的主编,也是文献[30]的收稿高级编辑(accepting senior editor)
Journal of the Association for Information Systems(2) Communication of the ACM(1) Information& Management (1) Decision Sciences(1) Decision Support Systems(1)	除了这几个期刊,关注信息安全比较多的还有 European Journal of Information System 和 Information System Journal 等,而专注于信息安全的期刊,如 Computer&Security 等多集中在功能范式,缺乏实证研究
管理科学(1)	国内研究信息安全管理的实证论文非常匮乏

资料来源:根据相关文献整理。

3 基于功能范式的研究

早期的信息安全管理研究绝大部分集中在功能范式,例如:应用最广泛的风险管理和最佳实践。信息安全风险管理最早开始于检查表,这在机器集中时代是可行的方法,由专家设计通用的检查表,系统管理员逐项核查,这种方法主要效仿自航空安全等传统领域的实践。但是计算机进入分布式计算时代,用户逐步从专业人员转向普通用户,检查表就不能应对这种情况了,第二代风险管理主要起源于经典六因素法,即:$R=f(A,T,V,C,L,I)$。风险是资产、威胁、脆弱性、控制措施、可能性和影响的函数,这个阶段的研究主要集中在可靠性、相关风险和流程设计等内容。而信息安全最佳实践是以一系列的规范作为代表的,例如,ISMS 和 COBIT③ 等。

除文献[8]外的基于功能范式的早期研究的共同特点是专注于解决现实中面临的问题,而不关注理论建构和实证,以信息安全意识培训为例,就有过程方法、社会工程方法和心理学方法等各种借鉴而来的功能范式的研究[9],因此,Puhakainen 和 Siponen[10]认为:几乎没有研究能够解释员工为什么会遵守安全策略,并提供相应的实证数据,因此信息安全意识培训亟须有理论基础的实证研究出现。

① ISMS,Information Security Management System,信息安全管理体系。ISMS 一般专门指 ISO/IEC 27000 标准族,该标准族囊括了 ISO/IEC 27000- ISO/IEC 27059 的 60 个标准,其中也包括比较常用的 GB/T 22080-2008 / ISO/IEC 27001:2005。由于其广泛的应用,目前以 ISMS 作为背景研究信息安全的论文比较多,例如:文献[1]和文献[11-12]。

② SOX,Sarbanes-Oxley Act,萨班斯-奥克斯利法案,全称为《2002 年公众公司会计改革和投资者保护法》(*Public Com-pany Accounting Reform and Investor Protection Act of 2002*),是美国政府根据安然(Enron)和世通(Worldcom)等财务欺诈事件破产暴露出来的公司和证券监管问题所立的监管法规,其中与信息安全相关的是涉及企业内部控制的条款 404。目前以 SOX 为背景研究信息安全的论文也很多,例如:文献[16]以及文献[19]。

③ COBIT,Control Objectives for Information and related Technology,即信息及相关技术的控制目标,COBIT 是 ISACA(信息系统审计和控制联合会)制定的面向过程的信息系统审计和评价的标准。

该文献应用了详尽可能性模型(Elaboration Likelihood Model,ELM)与通用建构指导模型(Universal Constructive Instructional Theory,UCIT),并通过行动研究(Action Research)进行了实证研究,这种介入性的研究方法表明了文献中所设计的培训规程对员工安全策略遵守(Policy Compliance)的正向影响作用。与之不同的是,Karjalainen 和 Siponen[9] 不但进行了实证研究,而且用元理论(Meta-Theory)试图找出信息安全培训的本质,这些理论如何影响培训效果以及安全培训与其他培训的本质不同之处。

正如 Dhillon 和 Backhouse[4] 所断言,随着数据的积累以及研究的深入,近几年基于功能范式的研究在顶级期刊上已经越来越少,而且有理论基础的实证研究多集中在以人员为研究核心的信息安全培训领域。基于功能范式的主要研究一览如表 2 所示。

表 2 基于功能范式的主要研究

文献(发表时间)	应用理论	主要研究结论/贡献
Karjalainen 和 Siponen[9](2011)	元理论	建构了信息安全培训元理论,并给出了四个示范性的设计和评价培训规程的要求
Puhakainen 和 Siponen[10](2010)	ELM 与 UCIT	利用 ELM 与 UCIT 所设计的信息安全培训课程可以提高员工遵守安全策略的程度
Straub 和 Nance[8](1990)	威慑理论	在实证数据的基础上给出了一个应如何发现计算机滥用事件(discovery of abuse incidents)以及处罚相应的作恶者(discipline of perpetrators)的模型

资料来源：根据相关文献整理。

4 基于诠释范式的研究

诠释范式并不是要解决是什么(What it is)的问题,而是从主观个体的角度去解释什么样(As it is)的问题。例如,在信息系统研究领域,研究以计算机为基础的信息系统应用的社会意义。

诠释范式是近几年仅次于激进人本范式的研究活跃领域。文献[11]和文献[12]都是以 ISMS 作为背景进行的研究,从不同的角度探讨了权利和政治在“制度化”(Institutionalization)过程中的作用。Backhouse 等[11] 应用权力回路(Circuits of Power)理论,以 ISO/IEC17799 为案例,从公司、行业、国家以及国际四个层次解释了权力和政治在信息安全管理国际标准产生、发展和扩散的过程中所起的作用。Smith 等[12] 在文献[11]的基础上运用典型行动研究(A Canonical Action Research)分析了权力、政治、以及文化等因素影响 ISO/IEC17799 在一个组织内部的部署过程。

被用于诠释范式的研究还有制度理论,制度压力(Institutional Pressures)最早用来解释企业同形(Isomorphism),之后被广泛地应用到各个研究领域,例如：在个人隐私研究领域用于 HIPAA(Health Insurance Portability and Accountability Act,美国医疗电子交换法案)的接受(Adoption),在信息系统研究领域用来解释信息系统的接受、内化(Assimilation)和扩散(Diffusion)等。Hsu 等[13] 利用韩国 140 家企业作为样本研究了制度压力对信息安全创新的接受和内化的影响路径上环境稳定性、竞争优势、资源获取能力、高管支持、IT 能力和文化适应性的调节作用。

此外,上市公司的信息披露在公司治理领域一直是研究热点,但是由于信息安全一般不在强制披露的内容之列,因此研究比较少见,目前只有文献[14]和文献[15]。Gordon 等[14] 利用美国 2000—2004 年上市公司作为样本,通过对年报做文本搜索,对信息安全披露与股价做回归分析,结果发现信息安全披露与股价之间存在正相关,这为上市公司的信息披露提供了很好的指导,该文献同时探讨了

影响信息安全披露的内生变量的作用，解释了上市公司为什么会主动披露一些信息安全事件等负面信息。Wang 等[15]也研究了公司年报中安全风险披露所导致的市场反应，还试图通过已有的信息安全披露建立决策树模型(Decision Ttree Model)来预测未来的安全风险。文献[16]的数据来源虽然不是上市公司的年报，但和文献[14-15]存在很大的相似之处。该研究以 SOX 404 为背景，探讨了企业内部控制报告中的主要 IT 控制漏洞和管理收益预测准确性之间的关系，将主要关注点放在更好的信息安全控制措施是否会产生更高质量的信息这个问题上。上述三个研究都试图解释信息安全对组织的作用及其作用机理。

脆弱性(Vulnerability，有时也译为漏洞)管理是信息安全管理的重要组成部分。如果将脆弱性的生命周期分为四个阶段：

(1) 黑客或安全从业人员发现脆弱性；

(2) 供应商开发对应的控制措施；

(3) 用户应用控制措施；

(4) 黑客利用该脆弱性。那么 Ransbotham 等[17]的研究定位在(4)，即：脆弱性及其控制措施公布之后的黑客攻击。文献[17]探讨了基于市场的脆弱性披露机制的有效性，并与 CERT① 行业或公众脆弱性披露的优缺点进行了对比。

基于诠释范式的主要研究一览如表 3 所示。

表 3 基于诠释范式的主要研究

文 献	应用理论	主要研究结论/贡献
Wang 等[15](2013)	信息传递理论 决策树模型	信息安全披露中的风险减缓框架(risk-mitigation themes)与未来安全漏洞公告(future breach announcements)联系比较低
Hsu 等[13](2012)	制度理论	环境稳定性、竞争优势、资源获取能力、高管支持、IT 能力和文化适应性对制度压力影响信息安全创新的接受和内化具有显著的调节作用
Li 等[16](2012)	信息传递理论	SOX404 内部控制更有效，无重大 IT 控制漏洞和实施了数据处理完整性(Data Processing Integrity)的企业，管理收益预测更准确
Ransbotham 等[17](2012)	创新扩散理论	如果脆弱性通过市场机制被披露，攻击将会大大减少，安全环境随之提升
Gordon 等[14](2010)	信息传递理论； 市场价值相关模型(Market-Value Relevance Model)	上市公司主动披露信息条目中包括信息安全内容与企业的市场价值正相关
Smith 等[12](2010)	权力回路理论	分析了权力、政治、规范、以及文化等因素影响 AS/NES17799：2001② 在 New South Wales(NSE) State Government，Austrilia 的部署过程
Backhouse 等[11](2006)；	权力回路理论	以 AS/NES17799：2001 为例，解释了国际标准的产生、发展和扩散过程

资料来源：根据相关文献整理。

① CERT，Computer Emergency Readiness Team，美国计算机应急响应中心，该机构会持续的发布脆弱性信息，中国的对应组织为 CNCERT(国家互联网应急中心，http://www.cert.org.cn)。

② AS/NES 17799：2001 是澳大利亚/新西兰国家标准，等同采用 ISO/IEC 17799：2001，该标准的最新版本为 ISO/IEC 27002：2005，在中国，被等同采用为 GB/T 22081-2008。ISO/IEC 27002：2005 和 ISO/IEC 27001：2005 是 ISO/IEC 27000 标准族最重要的两个标准，前者为实用规则，多用于部署过程，后者为要求，多用于认证过程。

5 基于激进人本范式的研究

激进人本范式的研究开始的比较早，Straub[18]从1990年就已经开始关注用户行为中的“计算机滥用”，但之后在这一领域并没有太多的实证研究，直到近几年信息安全管理得到越来越多的关注。

无论是在信息系统研究领域还是信息安全研究领域，激进人本范式都更注重对人的行为的研究，而不仅仅是设计技术架构或管理体系。例如，文献[19]和文献[1]都直接借用了信息系统研究中的“用户参与”(User Participation)的概念。用户参与与信息系统成功之间的关系是信息系统研究领域的研究热点之一，Spears和Barki[19]选择以SOX为背景，用定性和定量研究相结合的方法探讨了用户参与对信息安全意识、业务流程结合和安全控制开发等正向影响作用，谢宗晓等[1]则选择以ISMS作为背景，建立了用户参与通过信息安全意识和业务流程结合，最后影响信息安全管理有效性的多重中介模型。这两篇文献都驳斥了目前信息安全业界普遍持有的“人是信息安全体系中最薄弱的环节”的观点。

源于犯罪学、社会学和心理学的个体行为理论是近几年在研究安全策略遵守时应用的热点。文献[20-23]和文献[2-3]都应用了威慑理论(Deterrence Theory)。Herath和Rao[3]的研究结论与犯罪学保持了一致，即惩戒的确定性(Certainty of Sanction)降低犯罪率，但惩戒的严厉性(Severity of Sanction)对降低犯罪率没有显著影响。D'Aray等[23]采用实验方法探讨了三种安全控制措施：安全策略的用户意识(User Awareness of Security Policies)、安全意识培训与教育程序(Security Education Training and Awareness Programs)和计算机监控(Computer Monitoring)对惩戒的确定性以及惩戒的严厉性的影响，同时也验证了惩戒的确定性和惩戒的严厉性对信息系统误用意向(IS Misuse Intention)的影响，结果表明感知的惩戒严厉性与信息系统误用意向呈显著负相关。Siponen和Vance[22]用情景模拟法(Scenario Method)发现无论是正式的还是非正式的惩戒措施都不会降低员工违反安全策略的可能性。Hu等[2]的研究结果也表明惩戒的确定性、惩戒的严厉性和惩戒的敏捷性(Celerity of Sanction)对员工的安全策略遵守意向都没有显著的影响作用；Chen等[20]则是采用了一个新的视角应用威慑理论，即比较了奖励(Reward)、惩罚(Penalty)和控制措施确定性(Certainty of Control)对安全策略遵守的影响以及其交互作用。Guo和Yuan[21]验证了组织惩戒、工作组(Workgroup)惩戒和个体惩戒对安全策略遵守意向的影响及其交互作用。可见，虽然威慑理论在信息安全情境中有丰富的研究，但是惩戒的确定性和惩戒的严厉性对安全策略遵守意向的影响并没有确切的结论。

文献[24]应用了理性选择理论(Rational Choice Theory)。Bulgurcu等[24]认为信息安全意识会影响结果的信念(Beliefs about Outcomes)，进而影响整体的后果评估信念(Beliefs about Overall Assessment of Consequences)，最终影响个体态度直至遵守意向，该研究中将整体的后果评估信念用遵守的利益(Benefit of Compliance)、不遵守的代价(Cost of Noncompliance)和遵守的代价(Cost of Compliance)三个维度表征，并得出结论：遵守的利益和不遵守的代价对态度有显著正向影响，遵守的代价对态度有显著负向影响。

文献[22]还应用了中和理论(Neutralization Theory)。Siponen和Vance[22]选用了6个中和技巧：否认责任(Denial of Responsibility)、否认伤害(Denial of Injury)、否认必要性(Defense of Necessity)、谴责那些谴责他们的人(Condemnation of the Condemners)、高度效忠(Appeal to Higher Loyalties)和分类账隐喻①(the Metaphor of the Ledger)，并得出所有这些中和技巧对安全策略违反

① 分类账隐喻(The Metaphor of the Ledger)的基本含义是指个体相信自己所做的坏事能够被自己曾经所做的好事来抵销。

意向(Intention to Violate Is Security Policy)有显著的正向影响。

文献[25]以及文献[26]应用了保护动机理论(Protection Motivation Theory)。其中,Johnston和Warkentin[25]验证了感知的威胁严重性(Perceived Threat Severity)对自我效能(Self-Efficacy)和响应效能(Response Efficacy)都有显著负向影响,自我效能和响应效能对用户行为意向都有显著正向影响,但是感知的威胁易感性(Perceived Threat Susceptibility)对自我效能和响应效能影响均不显著。这个结论在Anderson和Agarwal[26]中的研究中也得到了相似的结论。

还有一些学者试图从个体特征探讨安全策略遵守意向。Hu等[2]验证了个体倾向(Individual Propensity),个体道德信念(Individual Moral Beliefs)与理性选择计算(Rational Choice Calculus),以及安全策略遵守意向之间的关系。Bulgurcu等[24]验证了规范信念(Normative Belief)对遵守意向的正向影响。

此外,信息安全策略违反或信息安全事件发生率的数据很难获取,导致对员工遵守信息安全策略的行为测量就比较困难,所以目前的相关研究一般会采用计划行为理论(Theory of Planned Behavior),用测量员工遵守信息安全策略的意向来代替策略遵守行为。例如:文献[3]、文献[24]以及文献[27-28]。

基于激进人本范式的主要研究一览如表4所示。

表4 基于激进人本范式的主要研究

文 献	应用理论	主要研究结论/贡献
谢宗晓等[1](2013)	用户参与理论	信息安全意识和业务流程结合在用户参与对信息安全管理有效性之间起中介作用
Chen等[20](2012)	威慑理论 服从理论	不但验证了奖励、惩戒以及安全控制确定性对策略遵守意向的作用,还验证了三个自变量之间的交互作用
Hu等[2](2011)	理性选择理论 个人控制理论 威慑理论	验证了个体倾向、个体道德信念、感知的威慑对理性选择计算及行为意向的影响
Guo和Yuan[21](2012)	威慑理论	组织惩戒会影响工作组惩戒和个体惩戒,但是不会直接影响遵守意向,工作组惩戒会影响个体惩戒,并显著负向影响遵守意向
Hu等[27](2012);	计划行为理论	将计划行为理论模型加入高层管理(Top Management)与组织文化(Organization Culture),建立个体行为模型,研究高层管理如何影响员工的安全遵守行为
Johnston和Warkentin[25](2010)	保护动机理论	恐惧诉求(Fear Appeals)会影响信息系统用户遵守安全策略的行为意向,其中恐惧诉求模型由保护动机理论而来
Anderson和Agarwal[26](2010)	保护动机理论	家庭计算机用户完成安全相关行为受认知、社会和心理等因素影响
Spears和Barki[19](2010)	用户参与理论	用户参与通过提高用户的安全意识、信息安全风险管理与业务环境的结合、控制措施开发促进安全控制绩效
Bulgurcu等[24](2010)	计划行为理论 理性选择理论	员工遵守安全策略的意向显著地受态度、规范信念和自我效能的影响
Siponen和Vance[22](2010)	中和理论 威慑理论	中和技巧对安全策略违反意向有显著正向影响,是开发信息安全策略和应用实践中的重要考虑因素
D'Aray等[23](2009)	威慑理论	三类安全实践可以有效威慑IT滥用行为:安全策略的用户意识、安全意识培训与教育程序和计算机监控对感知的惩戒确定性和感知的惩戒严厉性都存在显著正向影响

续表

文　献	应用理论	主要研究结论/贡献
Herath 和 Rao[3](2009)	威慑理论 计划行为理论 代理理论	个人安全行为会受到内部或外部因素的影响，个人规范与同伴(Peer)行为以及个人感知的有效性等对遵守安全策略的意向都有显著正向影响。此外，惩罚的确定性对遵守安全策略的意向有正向影响，但惩罚的严厉性影响不明显
Denev 和 Hu[28](2007)	计划行为理论	感知的控制措施易用性(Percieved Ease of Use)对行为意向和态度影响作用都不显著，感知的控制措施有用性(Percieved Usefulness)对行为意向作用不显著，但是对态度有显著正向影响
Straub[18](1990)	威慑理论	威慑管理规程(Deterrent Administrative Procedures)和安全预防软件(Preventive Security Software)都能够显著地降低计算机滥用

资料来源：根据相关文献整理。

6 基于激进结构范式的研究

和功能范式一样，激进结构范式也是基于客观视角的，但是认为结构是突变的，因此伴随着冲突和中断，基于激进结构范式的研究多致力与开发自圆其说的一整套体系，TQM、ISMS 和 COBIT 等框架都可以认为是激进结构范式的代表，为用户提供了一整套的解决方案，正如 ISO/IEC27001：2005 引文中所指出：本标准为实施 OECD① 指南中规定的风险评估、安全设计和实施、安全管理和再评估的原则提供了一个强健的模型。

基于激进结构范式的研究一直比较匮乏。Ransbotham 和 Mitra[29] 在综合了犯罪学的理性选择理论，差别接触理论(Differential Association Theory)，社会学习理论(Social Leaning Theory)，亚文化理论(Subculture Theory)，社会控制理论(Socail Control Theory)，受害者理论(Victim Theory)和组织犯罪理论(Organization Crime Theory)等基础上提出了信息安全策略妥协过程(Information Security Compromising Process，ISCP)的概念模型，Willison 和 Warkentin[30] 则在遏制—预防—检测—改进(Deterrence-Prevention-Detection-Remedies)基础上扩展设计了一个针对计算机滥用的安全行动模型。基于激进结构范式的主要研究一览如表 5 所示。

表 5　基于激进结构范式的主要研究

文　献	应用理论	主要研究结论/贡献
Willison 和 Warkentin[30](2013)	现有的在信息安全情境中应用过的诸多理论综合	以计算机滥用为关键点，按照时间序列给出了安全行动模型，其中包括 7 个步骤：组织与员工交互、组织不公及中和技巧、威慑、产生行动意向、预防(Prevention)、检测(Detection)和纠正(Remedy)未被检测到的滥用，并探讨了可能的 5 个研究领域
Ransbotham 和 Mitra[29](2009)	诸多犯罪学理论综合	设计了一个 ISCP 的概念模型

资料来源：根据相关文献整理。

① OECD，Organisation for Economic Cooperation and Development，经济合作与发展组织，简称经合组织，在 1990 年，OECD 公布了《信息系统安全指南》(*Guidelines for the Security of Information Systems*)2002 年改版为《信息系统与网络安全指南》(*Guidelines for the Security of Information Systems and Networks*)。

7 脉络梳理与研究展望

7.1 所有研究的脉络梳理

将文献分别按照时间—范式以及研究问题—范式来划分，统计数据如表 6 所示。

表 6 所有研究的脉络梳理一

	功能范式(3)	诠释范式(7)	激进人本范式(15)	激进结构范式(2)
2013(3)		Wang 等[15](2013)	谢宗晓等[1](2013)	Willison 和 Warkentin[30](2013)
2011-2012(8)	Karjalainen 和 Siponen[9](2011)	Hsu 等[13](2012)；Ransbotham 等[17](2012)；Li 等[16](2012)	Chen 等[20](2012)；Hu 等[2](2011)；Guo 和 Yuan[21](2012)；Hu 等[27](2012)	
2010(8)	Puhakainen 和 Siponen[10](2010)	Gordon 等[14](2010)；Smith 等[12](2010)	Johnston 和 Warkentin[25](2010)；Anderson 和 Agarwal[26](2010)；Spears 和 Barki[19](2010)；Bulgurcu 等[24](2010)；Siponen 和 Vance[22](2010)	
2009 及之前(7)	Straub 和 Nance[8](1990)	Backhouse[11]等(2006)	D'Aray 等[23](2009)；Herath 和 Rao[3](2009)；Denev 和 Hu[28](2007)；Straub[18](1990)	Ransbotham 和 Mitra[29](2009)

资料来源：根据相关文献整理。

注：a)MIS Quarterly 2010. 34(3)为信息安全专刊；b)功能范式数量众多，但多不符合筛选条件；c)表头括弧内为统计的文献数量。

表 7 给出了目前信息安全管理的研究问题与这四个范式的对应关系。

表 7 所有研究的脉络梳理二

基本范式	研究问题(部分)
功能范式	信息安全风险分析/评估/管理；信息安全最佳实践(其中包括很多，例如如何防止计算机滥用)；信息安全测量；信息安全培训
诠释范式	信息安全披露与股价的关系；制度压力对组织内部信息安全的影响；权力和文化等对信息安全标准部署的作用
激进人本范式	个体对信息安全策略的遵守行为；用户参与在信息安全管理中的作用
激进结构范式	ISMS(框架部分，不包括所有的标准)；COBIT；组织信息安全妥协过程；防止计算机滥用的行动框架

资料来源：根据相关文献整理。

在表 6 的统计中，功能范式的研究比较少，这是由于基于技术视角的功能范式多没有实证，不符合本文的筛选条件。事实上，通过表 7 可以看到，功能范式还是信息安全管理领域的研究热点，近几年功能范式的研究也还很多，但是绝大部分没有发表在表 1 所列的期刊上。激进人本范式的研究是

最近几年的热点，这主要是由于基于个体行为的理论比较成熟，很容易借鉴到信息安全情境中去。

7.2 目前研究的不足及展望

综上所述，心理学、社会学和犯罪学理论的应用一定程度上解决了Dhillon和Backhouse[4]所提出的实证研究缺乏理论基础的问题，但是目前的研究还存在诸多的不足之处，有待深化。

第一，理论建构远远不够，绝大部分研究集中在已有社会科学理论的简单应用，例如，Spears和Barki[19]虽然用定性和定量相结合的研究方式，即用定性方法提出研究假设，用定量方法进行了验证，但是基本沿用了信息系统研究领域的用户参与理论。更多的研究则是应用了犯罪学理论中个体行为的相关理论，如威慑理论和理性选择理论等。对比其他研究领域，信息安全有其特殊性，例如：便利性和安全性的矛盾，以IT解决IT安全所带来的额外风险；而且信息安全违规的受害者往往是组织，一般对作恶者形成不了实际的伤害，这导致信息安全策略更容易被违反等问题。在后续的研究中，应该更多应用行动研究、案例研究、民族志学(Ethnography)和扎根理论(Grounded Theory)等偏重建构理论的研究方法，关注信息安全的根本问题及其特殊性，建构信息安全管理理论。

第二，分析层次多集中在个体，应该多样化。既然约束个体行为的信息安全策略推动者是组织，隐含的含义是实现组织层次的信息安全更重要(上述研究中除了文献[26]，该文献关注家庭用户)，但是已有的研究多集中于个体对安全策略的遵守，绝大多数分析层次也都是个体层次，也就是说并没有解决最根本的问题，这也导致了忽略类似组织声誉、客户流失和财务状况等组织层次的影响因素[24]。此外，在已有的成熟研究中，普遍认为员工个体安全行为只是保障组织安全的一部分。因此，转向组织层次的研究是必要的。同样，基于工作组的分析层次也是有必要的。Guo和Yuan[21]构建了来自不同层次惩戒措施对安全策略遵守意向的影响模型也表明不同层次的信息安全控制存在交互作用。因此，在后续的研究中应该多关注组织层次和工作组层次的信息安全管理。

第三，样本单一，且多基于自报告(Self-reported)模式测量个体意向。目前绝大部分的研究都是采用美国公司员工或MBA作为研究样本，信息安全管理不可避免地受到文化、政治和法律等环境要素的影响，应该进行更多的跨文化研究，或者进行比较研究，例如：在集体主义文化和个人主义不同的文化环境下，同伴压力(Peer Pressure)对信息安全策略遵守的影响，或者在“关系”(GuanXi)文化中，惩戒的确定性和惩戒的严厉性对安全策略遵守意向的影响与制度比较完善的西方国家是否保持一致。在后续的研究中应该采用多样化的样本和数据来源，例如：可以考虑用组织积累的信息安全事件档案数据表征信息安全管理有效性，或者用第三方组织的客观评价数据表征信息安全管理有效性。

第四，目前研究集中在有限的几个问题，尤其是信息安全意识。信息安全管理包括一系列的控制点，ISO/IEC27001：2005的附录A就列出了11个安全域，39个控制目标，133个控制点，其中包括了信息安全意识，还包括了高管支持、安全组织和安全方针等更多的控制措施，例如：Ransbotham和Mitra[29]在概念模型中曾推测审计(Audit)不会直接影响ISCP，经过一段时间会提高其他控制措施的有效性，但没有跟进的实证研究。在后续的研究中应该关注更多的安全控制点，而不仅仅关注与个体行为联系紧密的信息安全意识。

7.3 几个深入研究的方向

根据现有研究的脉络梳理和目前研究中存在的不足，如下几个方面在后续的研究中应该关注或深入。

第一，基于多层次分析，深入探讨信息安全外部监管制度影响组织内部的信息安全管理的机制。信息安全往往面临着一系列的监管制度和强制标准，例如：公安部下发的信息系统安全等级保护，银

监会下发的信息科技风险管理指引等①。外部的制度压力对组织的信息安全管理有效性有多大的影响，通过什么机制影响到工作组，直至个体安全行为，这是需要深入研究的方向之一，其中研究内容也包括了 Ransbotham 和 Mitra[29]所提出的命题。

第二，平衡安全性和便利性的信息安全战略及其与信息系统战略以及组织战略的匹配(fit)问题。信息安全一般只会降低组织的潜在损失，而不会增加组织的盈利，因此，信息安全是成本效益分析下的安全，追求绝对的安全或过度的安全都是没有必要的。信息安全战略的设计必须考虑组织需要和目标、安全要求、业务过程、组织的规模和结构以及信息化水平等因素，力求做到与信息系统战略和组织战略相匹配。现有的研究没有关注信息安全安全性与便利性的矛盾，至于信息安全战略与信息系统战略以及组织战略的匹配问题的研究则更少。

第三，黑客和内部计算机犯罪的非主流群体的行为。由于样本的不易获取，现有研究中关于黑客的文献大多没有实证，这也导致 MIS Quarterly 在 2010 年编辑评论文章中就呼吁将研究方向转移到黑客和内部计算机犯罪的非主流群体中。事实上，绝大部分的计算机犯罪都与这个群体有关。但是到目前为止，仅有少量的文献以黑客社区网站为数据来源，通过社会网络的视角研究黑客行为，由于数据源很不精确等原因，关于黑客和内部计算机犯罪的高质量研究还是非常匮乏。

第四，信息安全管理制度化过程。已有信息安全管理制度/策略的研究，都放在了如何提高员工的遵守意向或改变员工态度等问题上，但是制度来自何处？制度是如何被建立的？制度推动者是谁？在组织内部，由于大部分的业务部门认为信息安全是信息技术部门的问题，而信息安全策略往往又降低了信息系统的便利性，因此对信息安全的管理制度抱有抵触情绪，信息安全制度/策略的产生过程往往伴随着各个部门权力博弈的过程。如何利用博弈论(Game Theory)观点研究信息安全管理制度化的过程应该引起关注。

第五，信息安全披露与公司市值/绩效之间的关系以及披露动机等需要继续深入。近几年，随着公众的关注，许多公司网站上陆续开始公布信息安全事件及处置措施，在上市公司年报中也开始进行信息安全方面的披露，现有的研究中只有文献[14-15]探讨了信息安全披露与公司市值之间的关系，但是什么原因导致了公司的信息安全披露行为？网站披露和公司年报披露对公司市值的影响有什么不同？这些问题在后续的研究中都应该继续深入探讨。

参考文献

[1] 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[J]. 管理科学，2013，26(3)：65-76.

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

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

[4] Dhillon G，Backhouse J. Current direction in IS security research：Towards socio-organizational pperspectives[J].

① 1994 年，国务院发布 147 号令，即《中华人民共和国计算机信息系统安全保护条例》，其中明确了“公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作”。之后公安部陆续出台一系列信息系统安全等级保护的公文和相关技术标准。例如：公通字[2007]43 号：关于印发《信息安全等级保护管理办法》的通知；GB 17859-1999《计算机信息系统安全保护划分准则》；GB/T 22239-2008《信息系统安全等级保护基本要求》GB/T 22240-2008《信息系统安全保护等级定级指南》等。银监发[2009]19 号：关于印发《商业银行信息科技风险管理指引》的通知。所有的规范性文件都可以在中华人民共和国中央人民政府网站(http://www.gov.cn/)或相关部委官方网站查阅。

Information Systems Journal,2001,11: 127-153.

[5] Siponon M T. Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods[J]. Information and Organization,2005,15(4): 339-375.

[6] Burrell G,Morgan G. Sociolgical Paradigms and Organization Analysis[M]. London: Heinemann,1979: 34-61.

[7] 罗珉.管理学理论范式述评[J].外国经济与管理,2006,28(6): 1-10.

[8] Straub D W, Nance W D. Discovering and disciplining computer abuse in organizations: A field study[J]. MIS Quarterly,1990,14(1): 45-60.

[9] Karjalainen M,Siponon M T. 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.

[10] Puhakainen P,Siponon M T. Improving employees' compliance through information systems security training: An action research study[J]. MIS Quarterly,2010,34(4): 757-778.

[11] Backhouse J, Hsu C W, Silva L. Circuits of power in creating de jure standards: Shaping an international information systems security standard[J]. MIS Quarterly,2006,30: 413-438.

[12] Smith S, Winchester D, Bunker D, Jamieson R. Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization[J]. MIS quarterly,2010,34(3): 463-486.

[13] Hsu C,Lee J N,Straub D W. Institutional influences on information systems security innovations[J]. Information Systems Research,2012,23(3): 918-939.

[14] Gordon L A,Loeb M P,Sohail T. Market value of voluntary disclosures concerning information security[J]. MIS Quarterly,2010,34(3): 567-594.

[15] Wang T,Kannan K N, Ulmer J R. The association between the disclosure and the realization of information security risk factors[J]. Information Systems Research,2013,24(2): 201-218.

[16] Li C,Peters G F,Richardson V J,Watson M W. The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports[J]. MIS Quarterly, 2012,36(1): 179-203.

[17] Ransbotham S,Mitra S,Ramsey J. Are markets for vulnerabilities effective[J]. MIS Quarterly,2012,36(1): 43-64.

[18] Straub D W. Effective IS security: An empirical study[J]. Information Systems Research,1990,1(3): 255-276.

[19] Spears J L,Barki H. User participation in information systems security risk management[J]. MIS Quarterly, 2010,34(3): 503-522.

[20] Chen Y,Ramamurthy K,Wen K. Organizations' information security policy compliance: Stick or carrot approach [J]? Journal of Management Information Systems,2012,29(3): 157-188.

[21] 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.

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

[23] 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.

[24] 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.

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

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

[27] Hu Q,Dinev T,Cooke D. Managing employee compliance with information security policies: The critical role of top management andorganizational culture[J]. Decision Sciences,2012,43(4): 615-660.

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

[29] Ransbotham S, Mitra S. Choice and chance: A conceptual model of paths to information security compromise[J]. Information Systems Research, 2009, 20(1): 121-139.

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

Information Security Management Research Review, Carding and Future Prospects

LIN Runhui[1] XIE Zongxiao[1] LIU Qi[2]

(1 Business shool of NanKai University, TianJin China, 300071

2 Department of information security, HeNan Police College, ZhengZhou, China, 450002)

Abstract With the application of IT degree rise, Information security has been received unprecedented attention. This article reviewed the existing information security management studies, in accordance with the management of the four basic paradigms: Functionalist paradigm, Interpretive paradigm, Radical humanist paradigm and Radical structuralist paradigm, and then followed the paradigm—Time and Paradigm—content on the main research conducted a carding, and finally summarizes the current deficiencies and gives in-depth research.

Key words Information Security, Information System Security, Management Paradigm

作者简介

林润辉(1972—),男,南开大学商学院,教授,博士生导师。研究方向:网络组织与治理、IT 项目管理、复杂管理系统分析、信息系统管理等。E-mail: linrh@nankai. edu. cn。

谢宗晓(1979—),男,南开大学商学院,博士生。研究方向:信息安全管理。E-mail: xiezongxiao@vip. 163. com。

刘琦(1978—),女,河南警察学院信息安全系,副教授。研究方向:密码学、信息安全。E-mail: 275645509@qq. com。