DOI: 10.16538/j.cnki.fem.2018.05.009

高管支持、制度化与信息安全管理有效性

董坤祥[1]，谢宗晓[2]，甄　杰[3]，林润辉[4]

（1. 山东财经大学 管理科学与工程学院，山东 济南 250014；2. 中国金融认证中心，北京 100054；
3. 重庆工商大学 商务策划学院，重庆 400067；4. 南开大学 商学院，天津 300071）

摘　要：为了探讨由企业高层管理团队推动的制度化是否可以提高信息安全管理有效性这一问题，本研究以国内通过信息安全管理体系认证的企业为调研对象开展问卷调查，采用PLS-SEM进行实证检验。研究发现：信息安全意识水平越高，高管支持（包括高管信念和高管参与两个维度）的程度越高，企业信息安全管理越有效；高管信念的强化，有助于提高信息安全制度中履行和内化的水平；制度化中的履行水平越高，企业信息安全管理越有效。本研究明确了企业内部提高信息安全管理有效性的路径，对于企业如何从制度视角推动信息安全管理实践具有重要的现实意义。

关键词：高管支持；信息安全意识；制度化；信息安全管理有效性

中图分类号：F270　**文献标识码：**A　**文章编号：**1001-4950(2018)05-0113-14

一、引　言

现阶段，信息安全已经得到了前所未有的重视。随着2014年2月“中央网络安全和信息化领导小组”的成立以及2017年6月《中华人民共和国网络安全法》的施行，信息安全在国家层面上得到了前所未有的重视。在组织研究领域和企业实践中，信息技术和信息系统的应用对企业发展的促进作用已经得到证明，信息已经成为企业的关键资产，关乎企业的生存和发展。然而，层出不穷的企业信息安全事件引起了公众和社会各界对于信息安全的关注和担忧，企业如何应对信息安全风险也成为近几年管理信息系统领域的研究热点。

收稿日期：2017-07-07

基金项目：国家社会科学基金青年项目（17CGL019）；国家自然科学基金面上项目（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）；山东省自然科学基金（ZR2017BG010）

作者简介：董坤祥（1988—），男，山东财经大学管理科学与工程学院讲师；
谢宗晓（1979—），男，中国金融认证中心信息安全服务部（通讯作者）；
甄　杰（1986—），男，重庆工商大学商务策划学院讲师；
林润辉（1972—），男，南开大学商学院教授，博士生导师。

企业信息安全风险主要源自员工的信息安全违规行为，制度化则是降低企业信息安全风险的有效途径。2016年国家计算机病毒应急处理中心的统计报告显示，2015年64.22%的被调查企业发生过信息安全事件。企业信息安全的威胁主要有两个：一是内部员工的违规行为，多方统计资料表明，70%—80%的信息安全问题源自员工无意的信息安全违规行为，例如设置简单的登录密码，随意点击含有钓鱼链接的邮件；二是企业外部威胁的入侵。主要包括黑客行为、网络间谍活动、有组织的犯罪以及网络恐怖主义等（赵衍，2013；陈昊等，2016）。事实上，员工的违规行为已经超越外部威胁成为企业信息安全风险的主要来源（D'Arcy等，2009；Bulgurcu等，2010；Boss等，2015），并且由于员工能够接触到企业的重要信息和数据，其信息安全违规行为的危害不容小觑（Hu等，2012）。因此，企业信息安全管理中一个亟待解决的现实问题是：如何通过制度的合理设计来规范和约束包含了硬件、软件和人员的整个企业信息系统，以减少信息安全事件的发生，提高信息安全管理的有效性。

信息安全制度化的开展需要企业高层管理团队的推动。企业信息安全管理是一项复杂的系统工程，它需要以信息技术部门为主，涉及多个相关职能部门，而信息安全制度的实施又与所有员工密切相关（Hu等，2012）。因此，只有作为对企业信息安全负有战略决策的高层管理者才有能力协调不同部门之间的关系，进而决定信息技术的引进、信息系统的部署以及信息安全制度的实施（武德昆等，2014；Barton等，2016）。由此可见，高层管理支持（简称"高管支持"）对企业信息安全制度的建设以及信息安全管理有效性的发挥有重要影响。然而，已有研究对于高管支持如何影响企业信息安全制度化，制度化过程对企业信息安全管理有何具体影响的探讨还远远不够。

探讨由企业高层管理团队推动的制度化是否可以提高信息安全管理有效性这一问题具有重要的理论和现实意义。有鉴于此，本研究以国内通过信息安全管理体系认证的企业为调研对象，探讨了高管支持、制度化与信息安全管理有效性之间的关系，旨在揭示高管支持如何推动了企业信息安全制度化，以及制度化对信息安全管理有效性有何具体影响，同时分析信息安全意识在此过程中的作用。本研究的理论贡献主要包括如下三方面：首先，与高管支持在企业国际化、公司创业、企业社会责任、安全策略遵守方面的研究相比（Carpenter等，2001；李华晶和邢晓东，2007；孙德升，2009；Hu等，2012），高管支持对企业信息安全制度化的影响一直被忽视。作为对这一研究不足的补充，本研究关注高管团队对信息安全管理重要性的认知和对信息安全管理活动的参与如何推动企业信息安全制度化，这对于理解为什么信息安全主管在企业高管团队中发挥重要作用有重要意义。其次，探讨了高管支持是否能够提高信息安全制度化水平。以往关于组织制度化的研究多是从外部环境的制度压力来展开，而较少涉及企业内部的高管支持。我们从企业内部分析影响信息安全制度化的因素，对于后续研究如何基于组织社会学的制度逻辑从企业内部和外部两方面来分析制度化过程具有借鉴意义。最后，探讨了信息安全意识对高管支持和信息安全管理有效性的影响。这对于明晰和构建企业信息安全制度化的内部传导机制具有启发性，并拓展了信息安全意识的影响范围和作用对象（Puhakainen和Siponen，2010），从而丰富了企业内部提高信息安全管理有效性的途径和方式。

二、理论基础与研究假设

（一）制度化

组织分析的新制度主义者强调"社会适当性"的重要性，认为组织所采用的结构形式应该是特定制度环境中不断寻求其合法性的结构形式。因此，组织的制度化是一个过程，它反映了组织适应外部环境的方式（Scott，2008）。Kostova和Roth（2002）根据组织制度具有合法性的特

点提出了制度化的两个过程：履行与内化，该研究是目前有关制度化大样本实证研究的典范，研究结论具有较好的普适性。

林润辉等（2016）在企业信息安全管理情境下对Kostova和Roth（2002）提出的履行和内化的制度化过程进行了重新阐述，并采用定量实证研究探讨了制度压力对履行和内化的影响。其中，履行是指组织对于自身制度化的外部表达，内化是指内部制度的真正付诸实施的过程（谢宗晓和林润辉，2016）。在企业信息安全实践中，最常见的关于制度化的外部表达方式就是设计满足外部监管要求的内部信息安全制度。由此可见，履行的过程更关注内部制度与外部制度和监管要求的一致性，内化的过程更偏重制度的实施，这种描述实际上与Kostova和Roth（2002）最初对履行和内化的定义保持了完全一致，只是将其在信息安全情境中进行了重新描述。因此，本研究沿用了Kostova和Roth（2002）和林润辉等（2016）提出和完善的履行和内化的制度化过程。

（二）高管支持与履行和内化

本研究认为信息安全管理情境下的高管支持，是指信息安全领导小组的成员（包括：CEO、信息安全主管、IT经理和业务经理）基于对企业信息安全管理重要性的认识，为了实现企业信息安全管理目标，向公司其他成员展现出的参与信息安全管理的态度和倾向性，以及参与信息安全实践行为的总和。它体现在信息安全领导小组成员对于信息安全管理的认知支持和行为支持，包括高管信念和高管参与两个维度（Hu等，2012；白海青和毛基业，2014；武德昆等，2014）。

在企业信息安全管理情境下，高管信念包括对企业信息安全管理重要性的看法、对信息安全管理的愿景规划、对信息安全管理成本的基本判断以及对信息安全管理相关知识的初步了解（武德昆等，2014）。基于该信念，企业高管会向其他管理者或人员传递信息安全重要性的关键信息，从而有力地推动企业各相关部门对于信息安全各类规范性文件的出台或发布，并在企业员工的日常管理中强调各类信息安全规范的落实（Warkentin和Willison，2009）。如此，便可以有效促进企业信息安全制度的外部表达和内部落实，使得信息安全管理有相应的制度化规范可以遵守。基于此，本研究提出如下假设：

H1：高管信念越强，制度化的履行水平越高。

企业中信息安全制度真正付诸实施就是内化的过程，也就是说，组织按照正式公布的文件建立信息安全协调机构的过程属于内化的范畴。企业的高层管理对于信息安全的重视和推动，能够构建一种信息安全管理的良好氛围，促使大家按照信息安全制度的要求进行规范化操作，进而减少企业内部信息安全事件的发生。可能的情况是，企业员工遵守信息安全管理策略所带来的收益可能不明显，但是一旦员工发生不遵守信息安全管理策略的不当行为所引发的事件便会给企业带来巨大的风险和损失。因此，本研究提出如下假设：

H2：高管信念越强，制度化的内化水平越高。

信息安全的制度化对于企业后续的一系列信息安全管理活动非常重要（Armstrong和Sambamurthy，1999；Sharma和Yetton，2003；Liang等，2007）。如果信息安全的制度化没有得到高管团队的参与和支持，制度化过程中所涉及的安全操作行为往往会被员工视作拖慢日常工作的额外工作负担（Hu等，2011）。因此，企业高层管理者对于信息安全制度化过程的参与和支持对于推动企业员工落实信息安全制度的各项工作有积极影响。

值得关注的是，高管参与可以有效协调来自不同部门之间的就执行信息安全相关措施所产生的冲突（Smith等，2010）。具体来说，高管参与到信息安全制度文件的制定中，从而实现以信息安全制度为基础的安全控制与不同部门业务流程的紧密结合（Spears和Barki，2010；谢宗

晓等，2013），强化企业对于信息安全制度化的外部表达；同时，高层管理者参与到企业内部信息安全策略的执行之中，会协调来自不同部门之间的利益冲突，推动信息安全的制度真正落实到员工的实际工作行为之中。因此，本研究提出如下假设：

H3：高管参与程度越深，制度化的履行水平越高。

H4：高管参与程度越深，制度化的内化水平越高。

（三）信息安全意识与高管支持和信息安全管理有效性

信息安全领域的研究表明，内部员工的不当行为所导致的信息安全事件已经成为了企业信息安全管理的主要威胁（D'Arcy等，2009；Herath和Rao，2009；Smith等，2010；Crossler和Johnston，2013）。因此，强化和提高内部员工的信息安全意识就显得尤为重要（Rezgui和Marks，2008）。ISF（information security forum）[①]将信息安全意识定义为组织内所有的员工理解信息安全的重要性，清楚组织所适用的安全级别，知悉并履行个人在日常工作中的安全职责（武德昆等，2014）。

Dinev和Hu（2007）分析了员工的技术意识对其信息安全保护行为的影响，结果表明员工的信息安全技术意识越高，越有利于其对企业信息安全的保护。Spears和Barki（2010）在企业信息安全风险管理的情境下，证明了员工参与信息安全活动能够显著提高其信息安全意识水平。Puhakainen和Sipone（2010）利用行动研究分析了信息安全意识培训对组织内部员工信息安全策略遵守行为的影响。结果表明，对组织员工的信息安全意识进行培训，可以显著提高其信息安全政策的遵守行为。谢宗晓等（2013）的研究结论则验证了员工信息安全意识对信息安全管理的有效性有显著正向影响，并在用户参与和信息安全管理有效性之间的关系中具有中介作用。基于上述分析，本研究提出如下假设：

H5：信息安全意识水平越高，企业信息安全管理越有效。

在实践中，微软公司在帮助客户建立信息安全方案的文献中也明确提出：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，从而改变全体员工的行为（武德昆等，2014）。与此相对应，Kruger和Kearney（2006）指出企业内部信息安全控制的效果依赖于积极的企业安全环境，其中包括每个人都理解并执行组织内的程序和规程，具有较高的信息安全意识。显然，对于高层管理来说，信息安全意识的提高有利于其在企业内部坚定地推广信息安全意识培训项目、执行信息安全管理政策以及建立纳入信息安全风险管理意识的企业文化（Rezgui和Marks，2008）。因此，信息安全意识的提高就会激励高管团队去积极的传播和参与到组织信息安全管理的活动中，进而发挥高管团队在信息安全管理中的有效作用。基于此，本研究提出如下假设：

H6：信息安全意识水平越高，高管信念越强。

H7：信息安全意识水平越高，高管参与程度越深。

（四）履行和内化与信息安全管理有效性

如前所述，履行是企业对于自身信息安全制度化的外部表达。在实践中，最常见的外部表达方式就是设计满足监管制度要求的内部制度。例如，有些行业监管机构要求企业必须有信息安全协调机构，其外在的表达方式就是公布各种正式或者非正式的相关文件。根据林润辉等（2016）的论述，企业信息安全制度化过程中的履行主要有三种类型：（1）为了满足监管或客户的要求；（2）响应各种协会的组织、宣传或获取补贴；（3）出于企业自发的安全需求。无论是哪种类型的履行都会不同程度地增加企业的管理规范性，直接或间接地提高企业的运维能力，最终会提高信息安全管理的有效性。基于此，本研究提出如下假设：

①ISF（https://www.securityforum.org）发布在信息安全实践中应用最为广泛的最佳实践。

H8：制度化的履行水平越高，企业信息安全管理越有效。

内化可以使信息安全管理的流程更加规范，规范的操作流程会降低可能的业务中断和企业遭受信息安全风险的可能性。尤其是信息安全管理的诸多研究已经表明，内部员工的信息安全违规行为已经成为企业信息安全风险的主要来源（Posey等，2014），而有效、规范的信息系统或信息技术操作流程，可以显著提高企业的信息安全水平（Boss等，2015）。换言之，良好的内化过程会使企业获得更高的信息安全有效性。因此，本研究提出如下假设：

H9：制度化的内化水平越高，企业信息安全管理越有效。

综上所述，本研究提出如下研究模型（见图1）。与已有研究比较，该模型做出了两点改进：第一，在企业信息安全管理情境下，明确了高管支持的两个维度。进一步分析高管信念和高管参与两个维度对制度化中履行和内化的影响路径和作用机制；第二，关注企业信息安全实践中信息安全管理有效性的问题。该模型突破了以往研究中重点探讨采纳行为实际发生前的影响因素和过程，而是从企业实践的管理层面上强调制度化过程对企业信息安全管理有效性的影响。

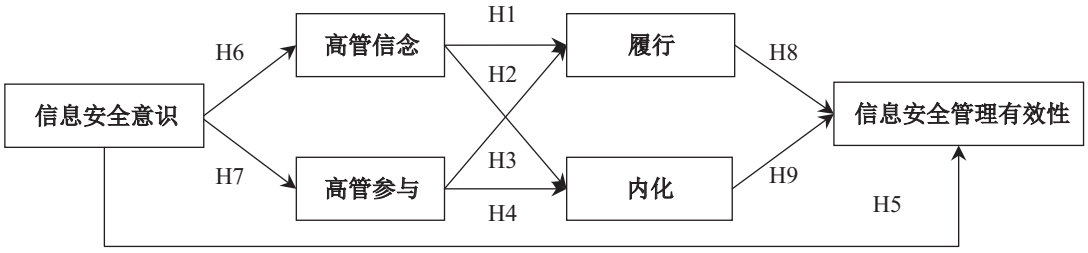


图 1　研究模型

三、研究方法

（一）样本选取与数据收集

本研究采用问卷调查法进行数据收集，调查问卷分为问卷A和问卷B。其中，问卷A的调研对象是通过GB/T22080-2008/ISO/IEC27001：2005[①]资格认证的企业组织中的相关管理者，受访者根据工作单位中信息安全制度的实施情况和信息技术、设备和信息系统的使用情况如实回答问卷中的问题；问卷B的调研对象是第三方认证机构[②]的审核员，受访者根据对应的标准来评价企业信息安全制度的部署情况以及实施后的绩效和效果。问卷A和问卷B均采用5点李克特量表（问卷A中1为很低，5为很高；问卷B中1为很差，5为很好），两个问卷中的量表均采用正向计分。

由于调查问卷分为问卷A和问卷B两部分，所以在数据获取过程中分为两个步骤：首先，通过电子邮件将问卷A发送给通过GB/T22080-2008/ISO/IEC27001：2005认证的企业相关管理者填写，共发送（文档版）电子问卷200份，回收有效问卷176份，问卷的有效回收率约为88%；其次，将收回的有效问卷交由负责第三方认证机构中审核目标企业的审核员进行填写，由于存在部分审核员离职等客观原因，造成部分问卷无法完成，因此回收到的有效问卷B为148份，问卷的有效回收率约为84%。

①GB/T22080-2008/ISO/IEC27001：2005这种标识的意思是GB/T22080-2008等同采用ISO/IEC27001：2005，即信息安全管理体系。《采用国家标准管理管理办法》中，第十五条 采用国际标准的我国标准的编号表示方法如下：（一）等同采用国际标准的我国标准采用双标号方法，实例：GB×××××-××××/ISO×××××：××××。（二）修改采用国际标准的我国标准，只使用我国标准编号。

②第三方认证机构指的是专门负责审核GB/T22080-2008/ISO/IEC27001：2005等标准的组织，国内有中国信息安全认证中心和中国电子技术标准化研究院等单位。虽然这次词汇来自ISO9000等管理体系标准审核，但是由于信息安全行业的特殊性，能够获取该资质的国内机构非常少。

（二）变量测量

本研究测量量表的所有题项均以已有研究中被广泛使用和验证的题项为范本，并结合本文的研究情境做出适当修改和调整。具体来说，高管支持包括高管信念和高管参与两个维度，对上述两个变量的测量采用Liang等（2007）的量表，均包括5个题项；对信息安全意识的测量根据Spears和Barki（2010）和D'Arcy等（2008）的量表改编得来，由4个题项构成，主要测量管理者对于信息安全必要性的认识；对制度化中履行和内化的测量采用Kostova和Roth（2002）、Hsu等（2012）和林润辉等（2016）的量表，均包括4个题项；对信息安全管理有效性的测量基于谢宗晓等（2013）和Chang和Lin（2007）的量表修改得来，由4个题项构成，1项测量机密性，1项测量可用性，1项测量完整性，1项测量企业信息安全管理的整体状况。所有变量测量的引用及设计说明，如表1所示。具体测量题项，请参见表2。

表 1　变量及其数据来源说明

潜变量	显变量	测量设计或说明	数据来源
高管支持	高管信念 高管参与	Liang等（2007） 武德昆等（2014）	问卷A（被试企业的管理者代表①填写）
制度化	履行 内化	以Kostova和Roth（2002）为基础的关键事件法	问卷B（负责被试企业ISMS审核的对应人员填写）
	信息安全管理有效性	谢宗晓等（2013） Chang和Li（2007）	问卷A
	行业类型 认证时间 组织成立年限 组织规模 IT部门规模 其他认证 所有制类型	控制变量，均来自客观数据	认证机构的档案数据 问卷A与认证机构的档案数据 网站信息

（三）控制变量

在控制变量方面，由于不同行业中的信息化发展水平不一致，进而造成不同企业对于网络依赖程度差异；成立时间和接受认证时间比较长的企业可能信息安全管理会更加规范，同时采用其他信息安全认证方式也会对企业的信息安全管理有一定影响；不同所有制类型的企业由于涉及关键信息的差异，会有不同的信息安全管理规范；组织规模和IT部门的规模也会对企业信息资产的规模有重要影响。基于上述分析，本研究将行业类型、所有制类型、组织成立时间、认证时间、有无其他认证、组织规模以及IT部门的规模作为控制变量，这与林润辉等（2016）和Hsu等（2012）等学者的研究相一致。

四、数据分析与结果讨论

大量实证研究已经表明PLS-SEM对样本数量没有严格限制，即使在样本数量有限的情况下仍然表现出良好的模型拟合效果（Reinartz等，2009）。由于本研究中的问卷A和问卷B的内容均涉及企业信息安全制度的实施情况，有可能会触及企业的敏感信息，所以导致问卷的回收数量相对较少，因此本研究采用PLS偏最小二乘法和Smart PLS 3.0进行数据分析。

（一）共同方法偏差

共同方法偏差（common method biases，CMV），是指由于同样的数据来源/评分者、同样的

①“管理者代表”是管理体系标准族中的专用名词，标准中要求管理者代表应该由组织的负责人或者分管领导担任。

表 2　问卷测量题项

变　量	题　项	数据来源
信息安全意识	1. 员工认为信息安全管理策略是必要的 2. 员工认为信息安全管理规范化是必要的 3. 员工认为信息安全管理的流程化是必要的 4. 员工认为安全意识培训程序(SETA. 是必要的	问卷A
高管信念	1. 高层管理认为信息安全可以保障组织信息资产不受损失 2. 高层管理认为信息安全会加强组织竞争力 3. 高层管理认为信息安全能够保证组织业务正常运营 4. 高层管理认为信息安全预算是组织战略投资的一部分 5. 高层管理认为信息安全控制会影响IT使用效率	问卷A
高管参与	1. 高层管理经常积极地阐明组织实施信息安全的重要性 2. 高层管理积极地主持制定组织的信息安全方针/战略 3. 高层管理积极地主持选择或制定信息安全策略 4. 高层管理经常积极地控制信息安全措施的实施过程 5. 高层管理经常积极地控制ISMS的监视与评审过程	问卷A
履行	1. ISMS部署文件包含了标准的所有要求 2. ISMS部署文件符合法律、法规和政策要求 3. ISMS部署文件要求与气压制度要求保持一致 4. 所有信息安全文件的要求是一致的	问卷B
内化	1. 结合组织的业务,识别了面临的信息安全风险 2. 对所识别出来的风险,进行了恰当的处置 3. 对所有控制措施运行情况,进行了监视和评审 4. 对所有的控制措施实施了有效性测量	问卷B
信息安全管理有效性	1. 降低了信息泄露的发生率及可能性 2. 降低了信息被篡改的发生率及可能性 3. 缩短了事件发生后恢复业务正常运行的事件 4. 提高了信息系统持续运营的能力	问卷A

测量环境和项目语境所造成的预测变量和效标变量之间人为的共变(周浩和龙立荣,2004)。这一问题在采用问卷调查法的研究中已经引起了学者们的广泛关注,所采用的控制方法主要是程序控制和统计控制两种。本研究中的数据来源构成包括问卷A和问卷B,且两部分问卷由不同类别的调研对象所完成,因此在程序控制环节有效避免了共同方法偏差的产生。而在统计控制方面,采用Harman单因素检验的方法进行验证。分析结果显示,所有变量的第一个因子的方差解释度为31.930%,小于40%的基准值。因此,本研究中所分析的数据不存在共同方法偏差的问题。

(二)测量模型检验

在对量表信度和效度进行检验的过程中,主要使用组合信度(CR)和项目载荷来评价量表的信度;主要用潜变量AVE(平均变异萃取量)的平方根是否大于潜变量之间的相关值来检验区分效度,用AVE来评价量表的聚合效度(Peng和Lai,2012;林润辉等,2016)。测量量表不同指标的结果详见表3和表4。

由表3可知,信息安全意识、高管信念、高管参与、履行、内化和信息安全管理有效性的组合信度(CR)分别为0.814、0.873、0.928、0.857、0.911和0.923,均大于0.700的基准值;6个潜变量的AVE分别为0524、0.579、0.721、0.603、0.720和0.749,均大于0.500的基准值;6个潜变量所有项目的因子载荷值均大于0.600,在可以接受的范围之内;6个潜变量中Cronbach's α的最小值为0.714,均在0.700以上。上述多个指标均说明了研究量表具有较好的信度水平。

表 3　测量量表信度和效度评价指标

构　念	题　项	因子载荷	T值	AVE	CR	Cronbach's α
信息安全意识	信息安全意识1	0.754	14.697	0.524	0.814	0.714
	信息安全意识2	0.742	12.540			
	信息安全意识3	0.749	8.418			
	信息安全意识4	0.647	5.520			
高管信念	高管信念1	0.786	27.982	0.579	0.873	0.821
	高管信念2	0.836	31.762			
	高管信念3	0.716	14.062			
	高管信念4	0.729	17.718			
	高管信念5	0.745	20.009			
高管参与	高管参与1	0.871	41.283	0.721	0.928	0.903
	高管参与2	0.871	40.636			
	高管参与3	0.839	30.896			
	高管参与4	0.843	33.735			
	高管参与5	0.821	26.734			
履行	履行1	0.854	20.080	0.603	0.857	0.773
	履行2	0.882	27.197			
	履行3	0.664	9.026			
	履行4	0.683	11.565			
内化	内化1	0.917	12.824	0.720	0.911	0.869
	内化2	0.885	10.844			
	内化3	0.791	8.886			
	内化4	0.792	8.891			
信息安全管理有效性	信息安全管理有效性1	0.902	45.572	0.749	0.923	0.888
	信息安全管理有效性2	0.866	26.292			
	信息安全管理有效性3	0.829	20.980			
	信息安全管理有效性4	0.865	36.553			

表 4　潜变量均值、方差和AVE的平方根

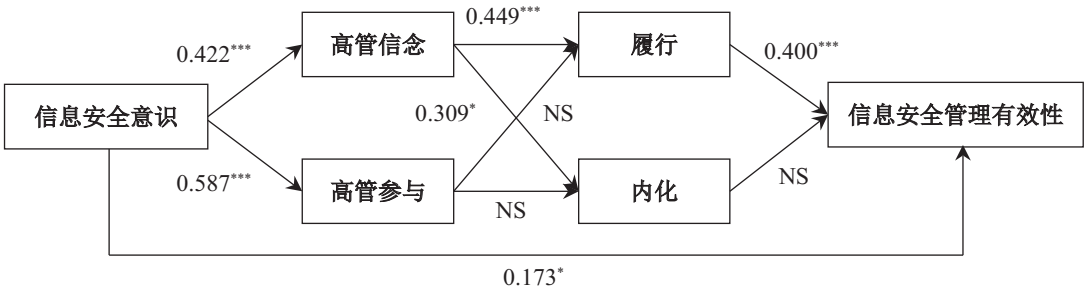
	(1)	(2)	(3)	(4)	(5)	(6)
(1)信息安全意识	0.724					
(2)高管信念	0.421	0.764				
(3)高管参与	0.583	0.625	0.849			
(4)履行	0.029	0.391	0.305	0.777		
(5)内化	0.071	0.212	0.139	0.413	0.848	
(6)信息安全管理有效性	0.179	0.422	0.472	0.440	0.238	0.866

由表4可知，6个潜变量的AVE的平方根均大于潜变量之间的相关系数，表明量表具有较好的效度。基于上述分析结果，本研究中的量表具有较高的可靠性和有效性。

本研究还按照Gefen等（2000）和Hu等（2012）等学者的建议，对交叉载荷做出了比对。结果显示（限于篇幅，未报告），项目载荷在设定的潜变量的数值要明显高于其他潜变量的数值，进一步证明了本研究量表具有良好的聚合效度和区分效度；对7个控制变量（行业类型、组织规模、认证时间、所有制类型、IT部门规模、组织成立时间和有无其他认证）纳入模型进行检验时，由于控制变量的数量较多，而所分析的样本量相对较少，因此借鉴了Liang等（2007）的分析方法而进行了7次检验，每次检验分别只涉及一个控制变量，由此可知（限于篇幅，未报告），7个控制变量的系数均不显著，即控制变量没有对模型的有效性产生影响。

（三）研究假设检验

假设检验的结果如图2所示。



注：*表示$p<0.05$，**表示$p<0.01$，***表示$p<0.001$。

图 2　假设检验结果

1. 信息安全意识对高管支持、信息安全管理有效性的影响

假设检验结果显示，信息安全意识对信息安全管理有效性有显著正向影响，因此假设H5得到验证（$\beta=0.173$，$p<0.05$）。该结果说明信息安全意识的提高，能够显著提高信息安全管理的有效性。信息安全意识对高管信念和高管参与均有显著正向影响，因此假设H6（$\beta=0.422$，$p<0.001$）和假设H7（$\beta=0.587$，$p<0.001$）得到验证，这就表明了良好的信息安全意识水平会确保高层管理人员对信息安全管理活动的重视和参与水平。该结果与Puhakainen和Siponen（2010）的研究结论基本一致，也为在企业信息安全实践中强调高层管理人员的思想重视和行动参与提供了实证依据。

2. 高管信念对履行和内化的影响

假设检验结果显示，高管信念对履行和内化均有显著正向影响，即假设H1（$\beta=0.449$，$p<0.001$）和H2（$\beta=0.309$，$p<0.05$）得到验证。上述结果表明，高层管理人员对信息安全活动的重视，能够促进企业内部信息安全制度的外部表达，即企业所发布的信息安全制度文件能够满足各项外部监管的要求。此外，高层管理人员对信息安全活动的重视，可以发挥良好的带动和示范效应，减少信息安全制度实施中的阻力，确保各项制度准则的顺利实施。

3. 高管参与对履行和内化的影响

假设检验结果显示，高管参与对履行和内化没有显著正向影响，假设H3（$\beta=-0.057$，$p>0.05$）和H4（$\beta=-0.112$，$p>0.05$）没有得到验证。该结果说明，高管参与对制度化没有显著促进作用，这与我们的预期假设出现了偏差，这可能是由于高层管理人员在信息安全活动中表现出的积极行为，与企业员工在日常工作中对制度的执行出现了偏差。换句话讲，高层管理人员没有办法接触和理解一般企业员工所感知到的信息系统的脆弱性和信息策略遵守行为给他们工作所带来的压力（Posey等，2014）。因此，只有高层管理人员和企业员工的信息安全行为完全一致时，才能有效发挥高管支持的正向引导和示范作用。

4. 履行和内化对信息安全管理有效性的影响

假设检验结果显示，假设H8得到验证（$\beta=0.400$，$p<0.001$），即履行对信息安全管理有效性有显著正向影响。出乎意料的是，内化对信息安全管理有效性没有显著正向影响，假设H9没有得到验证（$\beta=0.083$，$p>0.05$）。假设H8和H9所呈现的结论值得与林润辉等（2016）的研究发现进行对比。在本文中，因变量为涵盖机密性、完整性和可用性的信息安全管理有效性，而林润辉等（2016）的因变量为范畴更为广泛的信息安全绩效，包括竞争优势、经济效益和运维效率。对比两项研究中履行和内化对因变量的不同影响，可以在后续研究中深化研究制度化中履行和内

化对信息安全管理有效性的影响过程，分析假设H9没有得到验证的深层原因。

表5列出本研究中所有假设的路径系数、T值和假设检验的结果。

表 5　假设检验结果

假　设	路径系数	T值	结　论
H_1：高管信念→履行	0.449***	3.679	支持
H_2：高管信念→内化	0.309*	2.149	支持
H_3：高管参与→履行	–0.057	0.400	不支持
H_4：高管参与→内化	–0.112	0.829	不支持
H_5：信息安全意识→信息安全管理有效性	0.173*	2.255	支持
H_6：信息安全意识→高管信念	0.422***	6.938	支持
H_7：信息安全意识→高管参与	0.687***	12.419	支持
H_8：履行→信息安全管理有效性	0.400***	4.066	支持
H_9：内化→信息安全管理有效性	0.083	0.812	不支持

注：*表示p<0.05，**表示p<0.01，***表示p<0.001。

五、研究结论与展望

（一）研究结论

本研究在企业信息安全管理情境下，探讨了高管支持、制度化和信息安全管理有效性之间的关系。以国内通过信息安全管理体系认证的企业为调研对象，收集了148份有效问卷，采用结构方程模型对研究模型进行统计分析和实证检验，得出以下三点结论：信息安全意识的提高不仅能促进高管团队对信息安全的支持，而且还可以提高信息安全管理的有效性；高管团队对信息安全重要性的认知水平越高，越有利于企业信息安全制度化中履行和内化相关管理活动的开展；企业内部信息安全制度的落实水平越高，越有利于信息安全管理有效性的发挥。

以下对研究结论做进一步讨论。首先，信息安全意识能够提高高管支持的水平，提高企业信息安全管理的有效性。信息安全意识是对信息安全管理相关知识的认知，它可能来自于生活或工作的经验（如遭受过黑客攻击，接受过违反信息安全策略的处罚），也可能来自于外部环境的影响（如接受过信息安全培训）。在企业信息安全管理中，信息安全意识会不断纠正高层管理团队对信息安全活动的认知，以减少企业信息资源可能遭受的各种内外威胁。此外，信息安全意识遵循知识→劝说→决策的影响传递路径（Bulgurcu等，2010），因此信息安全意识的提高会影响高层管理团队对信息安全的态度，最终促进他们参与到信息安全管理活动中去。同样，良好的信息安全意识会积极影响企业员工日常的工作行为（如遵守信息安全管理策略），这也能够有效降低员工违规所引发的信息安全风险，提高信息安全管理的有效性。

其次，高管信念对履行和内化的正向影响深化了我们对高管团队与信息安全制度化之间关系的认识。一方面，企业的生存和发展需要遵循既定的社会标准和法律制度，进而获得其合法性。高层管理团队对于信息安全管理的认可以及对信息安全管理重要性的认知，可以推动企业对自身制度化的外部表达，实现制度化履行阶段的同时满足其外部合法性的要求；另一方面，企业高层管理团队对信息安全管理活动重要性的认知可以减少制度化内化阶段中的阻力，加速各项信息安全措施的实施和部署，保证内化阶段的顺利完成。

最后，履行对企业信息安全管理有效性的正向影响拓展了我们对信息安全制度化效用的理解。该结论所隐含的内在逻辑是，企业对自身信息安全制度的外部表达的准确性影响了信息安全管理活动的效果。企业设计满足外部监管要求的信息安全制度，这就意味着该制度所涵盖的价值体系在企业内部是正当且合理的。在这样的内部制度环境下，无论是企业的内部员工，

还是高层管理人员追求信息安全管理的策略和方法均会得到普遍认可。因此，在高层管理团队的示范和带动效应，以及员工的信息安全遵从同伴效应共同作用下，企业可以有效减少各类信息安全风险，提高信息安全管理的有效性。

（二）管理启示

本研究对企业如何推动信息安全管理有四个方面的启示。第一，加强企业员工和高层管理团队的信息安全教育，尤其是要培养和提升企业所有人员的信息安全意识。例如，在企业信息安全管理中构建完善的信息安全意识培训程序，帮助员工掌握合理的信息系统操作规范和应对信息安全风险的基本技巧。与此同时，如果企业的高层管理团队中没有信息安全主管或相对应的职位，应该针对此类高层管理团队开展定期的信息安全知识分享和教育活动，以保证高层管理团队成员具有良好的信息安全意识。第二，企业高层管理团队要足够重视信息安全制度化过程。高层管理团队对企业信息安全制度建设过程的关注和参与，能够有效促进企业在制度和流程上对信息安全进行合理设计，对包含了信息系统、信息技术、硬件、软件和员工的企业信息资源系统进行规范和约束，减少信息安全风险的发生。第三，企业的信息安全制度化需要有准确的外部表达，在获得合法性的同时确保信息安全管理的有效性。在企业公布的信息安全相关文件中要确保所有条款满足外部监管的要求。同时，所公布的组织正式文件要涉及企业信息资源的机密性、完整性和可用性，最大限度提高信息安全管理的有效性。第四，企业信息安全的获得不能仅仅依靠技术支持或系统升级，还需要在管理层面上采取合理的制度管理和控制。例如，注重对所有员工的信息安全意识培训，以日常工作为标准构建不同安全级别的员工系统登录权限，强化员工的信息安全策略遵守行为。也就是说，有效的信息安全管理手段均应该纳入信息安全制度相关文件，以保证企业信息安全管理活动的可行性和有效性。

（三）研究局限与未来展望

本研究还存在一定的局限性。首先，将高管支持划分为高管信念和高管参与两个维度，但是企业信息安全管理情境下高管支持的维度可能更为复杂。例如，企业高管团队中信息安全经理对于信息安全知识的分享，同样能够推动信息安全实践的开展。然而，在当前企业实践中，信息安全管理还没有得到足够的重视，这种信息安全知识的分享和传播机制还没有充分展开。随着企业信息安全管理实践的深入，后续研究应该从更多维度对高管支持进行结构化分析，这有助于发挥高管支持在信息安全管理中的积极作用。其次，没有考虑组织外部环境因素对企业信息安全制度化的影响。新制度主义学者强调制度的社会适当性，因此未来研究需要考虑外部制度压力等因素对企业信息安全制度化的影响过程，以丰富本文仅从内部管理视角探讨制度化影响因素的研究。最后，假设检验的结果显示高管参与对履行和内化的影响不显著，这与最初的研究假设出现了偏差。未来研究中需要深入探讨高管参与对履行和内化影响不显著的深层原因，这对于如何通过高管支持来持续推进企业信息安全的制度化可能会更有参考价值。

主要参考文献

[1]白海青, 毛基业. 高层管理支持信息系统的概念及维度研究[J]. 管理评论，2009, (10): 61-69.

[2]白海青, 毛基业. CEO支持信息化的动因: 激发条件与促进机制[J]. 南开管理评论，2014, (6): 114-125.

[3]李礼, 张延林, 张梦华. 高管支持行为细分——企业IT应用中信任作用的实证检验[J]. 管理科学，2010, (4): 68-76.

[4]林润辉, 谢宗晓, 王兴起, 等. 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[J]. 管理世界，2016, (2): 112-127.

[5]孙德升. 高管团队与企业社会责任: 高阶理论的视角[J]. 科学学与科学技术管理，2009, (4): 188-193.

[6]谢宗晓. 信息安全管理体系实施指南[M]. 北京: 中国标准出版社, 2012.

[7]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, (3): 65-76.
[8]谢宗晓, 林润辉. 信息安全制度化3I模型[J]. 中国标准导报，2016, (6): 30-33.
[9]张建君, 李宏伟. 私营企业的企业家背景、多元化战略与企业业绩[J]. 南开管理评论，2007, (5): 12-25.
[10]周浩, 龙立荣. 共同方法偏差的统计检验与控制方法[J]. 心理科学进展，2004, (6): 942-950.
[11]Barton K A, Tejay G, Lane M, et al. Information system security commitment: A study of external influences on senior management[J]. Computers & Security，2016, 59: 9-25.
[12]Boss S R, Galletta D F, Lowry P B, et al. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors[J]. MIS Quarterly，2015, 39(4): 837-864.
[13]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.
[14]Carpenter M A, Fredrickson J W. Top management teams, global strategic posture, and the moderating role of uncertainty[J]. Academy of Management Journal，2001, 44(3): 533-545.
[15]Chang S E, Lin C S. Exploring organizational culture for information security management[J]. Industrial Management & Data Systems，2007, 107(3): 438-458.
[16]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.
[17]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.
[18]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.
[19]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 Science，2012, 43(4): 615-660.
[20]Hsu C, Lee J N, Straub D W. Institutional influences on information systems security innovations[J]. Information Systems Research，2012, 23(2): 918-939.
[21]Kostova T, Roth K. Adoption of an organizational practice by subsidiaries of multinational corporations: Institutional and relational effects[J]. Academy of Management Journal，2002, 45(1): 215-233.
[22]Kruger H A, Kearney W D. A prototype for assessing information security awareness[J]. Computers & Security，2006, 25(4): 289-296.
[23]Liang H G, Saraf N, Hu Q, et al. Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management[J]. MIS Quarterly，2007, 31(1): 59-87.
[24]Peng D X, Lai F J. Using partial least squares in operations management research: A practical guideline and summary of past research[J]. Journal of Operations Management，2012, 30(6): 467-480.
[25]Posey C, Roberts T L, Lowry P B, et al. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders[J]. Information & Management，2014, 51(5): 551-567.
[26]Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: An action research study[J]. MIS Quarterly，2010, 34(4): 757-778.
[27]Reinartz W, Haenlein M, Henseler J. An empirical comparison of the efficacy of covariance-based and variance-based SEM[J]. International Journal of Research in Marketing，2009, 26(4): 332-344.
[28]Rezgui Y, Marks A. Information security awareness in higher education: An exploratory study[J]. Computers & Security，2008, 27(7-8): 241-253.
[29]Scott W R. Institutions and organizations: Ideas and interests[M]. 3rd ed. Los Angeles: Sage Publications, 2008.
[30]Sharma R, Yetton P. The contingent effects of management support and task interdependence on successful information systems implementation[J]. MIS Quarterly，2003, 27(4): 533-556.
[31]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[J]. MIS Quarterly，2010, 34(3): 463-486.
[32]Spears J L, Barki H. User participation in information systems security risk management[J]. MIS Quarterly，2010, 34(3): 503-522.
[33]Tyler T R, Blader S L. Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings[J]. Academy of Management Journal，2005, 48(6): 1143-1158.
[34]Tyler T R, Callahan P E, Frost J. Armed, and dangerous(?): Motivating rule adherence among agents of social control[J]. Law & Society Review，2007, 41(2): 457-492.
[35]Warkentin M, Willison R. Behavioral and policy issues in information systems security: The insider threat[J]. European Journal of Information Systems，2009, 18(2): 101-105.

Top Management Support, Legitimation, and Effectiveness of Information Security Management

Dong Kunxiang[1], Xie Zongxiao[2], Zhen Jie[3], Lin Runhui[4]
(1. *School of Management Science and Engineering*, *Shandong University of Finance and Economics*, *Ji'nan* 250014, *China*；2. *China Financial Certification Authority*, *Beijing* 100054, *China*；
3. *School of Business Planning*, *Chongqing Technology and Business University*, *Chongqing* 400067, *China*；
4. *Business School*, *Nankai University*, *Tianjin* 300071, *China*)

Summary: With increasing dependence on information technology and information system, enterprises are confronting with a more and more complicated information security environment. Thus, information security has become an intractable problem for many enterprises. Generally speaking, there are two methods to improve enterprises' information security level, that is, technology and management means. Technology means mainly settle software and hardware security of computers and networks, while management means mainly regulate and restrain the entire enterprise system including software, hardware, and employees. At present, a lot of enterprises mostly employ the technology means to solve information security problems. However, the lack or imperfection of information security institutions leads to bad enterprise information security situation. Therefore, technology and management means to solve information security are complementary to each other. As such, it is urgent and necessary to establish and improve information security institutions for many enterprises.

In fact, enterprise information security is a complicated activity which needs different sectors to get involved in. More specifically, the information security departments play the very critical role in the implementation of information security institutions, and all employees should comply with the information security policy. Therefore, only the top management teams have the ability to coordinate the relationship between different departments, determine the introduction of information technology, and deploy the information systems. In response, top management support has an important impact on the construct of information security institutions and the effectiveness of information security management. So far, few studies have investigated the mechanism that how top management support affects information security legitimation, and legitimation information security management. Therefore, it has great theoretical and practical significance to the exploration of whether the legitimation supported by top management can improve the effectiveness of information security management.

The objective of the current study is to explore whether legitimation prompted by top management team can improve the effectiveness of enterprise information security management. By doing so, the data was collected from the enterprises which have passed the certification of information security management system, and analyzed by using PLS-SEM. The results indicate that information security awareness can improve top management support(including top management belief and top management participation)and the effectiveness of information security management respectively. In addition, top management belief can improve implementation(the first stage of legitimation)and internalization(the second stage of legitimation). Moreover, implementation can improve the effectiveness of information security management. This paper analyzes the way to enhance effectiveness of information security management, which has a reality-oriented meaning for prompting information security management of enterprises from the standpoint of institution.

Key words: top management support; information security awareness; legitimation; effectiveness of information security management

（责任编辑：子　文）

(上接第15页)

process in modern Austrian school consists of three key interrelated analytical concepts: (a)the entrepreneur role; (b)the role of discovery; (c)adversarial competition. According to Hayek's divided knowledge theory, an entrepreneur's knowledge is individual, situational and implicit, and such rich personal knowledge means potential creativity, helping the entrepreneur discover and exploit opportunities. So based on Austrian school's ideas, Scott A. Shane created a conceptual framework of entrepreneurial research, induced scholars to concern with three sets of research questions about entrepreneurship: (1)why, when, and how opportunities for the creation of goods and services come into existence; (2)why, when, and how some people but not others discover and exploit these opportunities; (3)why, when, and how different modes of action are used to exploit entrepreneurial opportunities. Third, Scott A. Shane is a uniquely complete entrepreneurship scholar. He has made substantial contributions to the field of entrepreneurship. They can be summarized as follows: (a)he has strongly influenced what we view as central aspects of entrepreneurship, and has been a leading figure in redirecting the focus on entrepreneurship research itself; (b)he has influenced how we view entrepreneurship phenomenon by making full arguments and presenting theoretical insights; (c)in particular, he has emphasized the need to consider variation in the opportunities alongside the characteristics of those individuals who pursue them, as well as the matching of individuals and opportunities; (d)he has contributed to how we conduct entrepreneurship research; Scott A. Shane has been a forerunner of examining relevant units of analysis that are difficult to sample, designing entrepreneurial process research, processing data, and introducing sophisticated analytical methods; (e)he has laid the theory foundation of entrepreneurship and promoted the development of entrepreneurship.

Key words: entrepreneurial opportunity; entrepreneurial process; theoretical development; methodology

（责任编辑：墨　茶）