试论商业银行人员安全性控管:ISO17799 的借鉴与启示

浙江大学管理学院 辛金国 范 炜 浙江工业大学经贸管理学院 林素燕

[摘要] 信息安全是商业银行持续经营的生命所在。没有安全型的职员,就不可能保证企业的信息资产安全。借鉴 ISO17799 人员安全实施指南,为防范员工道德风险,确保资产安全,商业银行必须强化人员安全控制机制,并不断完善组织的内部控制。

[关键词] 人员安全,内部控制,ISO17799,信息安全

信息安全是当今信息社会非常重要的问题。然而,没有安全型的员工,就难于保证企业的实体资产和信息资产安全。人员安全性(Personnel Security)控管是企业内部控制的重要组成部分,建立人员安全性机制旨在降低人为错误、盗窃、诈骗和误用设备的风险[1]。

一、问题提出

近年来,由银行内部人员道德风险引发的信息安全(information security)事件在海外频频发生。今年 4 月 28 日,我国台湾《苹果日报》报道,由于不肖员工勾结骗徒,台湾五家银行客户资料被盗,近千万人资料外泄。2001 年,美国金融业因内部特殊"金融隧道"泄密,导致信用卡盗窃,损失的金额高达 15 亿美元。2002 年,美国个人信息被恶意利用的受害者多达 50 万人[2]。英国的一份官方统计报告《2002 年信息安全入侵调

量大,因此投资者在市场下降时卖出股票以防被深度套牢的欲望会比市场上升时买进以获取更大收益的欲望更强烈。另外由于过度反应的作用,由此可见,正是由于投资者对损失和收益进行权衡时对待损失和收益的态度的明显差异导致了羊群行为。

中国大陆和台湾的广大投资者无论从文化背景还是价值取向的一致性,使得两岸的投资者具有一些共同的特点:一方面两岸的股票市场都是散户居多,由于信息披露不完全,容易产生较多的"噪音交易者";另一方面在厌恶风险,又有追逐高风险从而获得高收益,而一夜之间暴富的心态。在股市上涨时,这些"噪音交易者"在过度反应理论中正反馈机制的作用下,大量买进,导致市场上的需求量增加,使得股市中呈现出"追涨"的现象。但当股市下跌时,由于前景理论中投资者对损失的厌恶,当股市稍有下跌,尤其是跌到投资者个人的"参考点"以下时,就可能导致大量抛售股票的行为,由于价值函数这种特殊的"S 形"形状,股票下跌的速度可能会非常快,所以会出现"杀跌"的倾向强于"追涨"的倾向,形成这种特殊的羊群效应是理所当然的。台湾股市虽然比大陆股市发展要早,但总体仍处于发展和完善阶段,由于投资者构成和价值取向的一致性,产生与大陆股票市场基本一致的羊群行为也就不足为奇了。

六、小结

羊群行为是金融市场上的普遍现象,无论在中国大陆的证券市场还是在台湾的证券市场,由于信息不对称较西方成熟市场更为严重,市场中的羊群行为也更为明显,这也是中国大陆和台湾证券市场过度波动的主要原因。从上述行为金融学的理论解释看,主要是由于在信息不对称情况下,个人投资者的理性选择就是观察他人的投资行为并模仿,而且许多投资者普遍存在赌博和暴富心理的偏差,从而产生了羊群行为;而机构投资者虽然具有信息优势,但由于委托代理人问题,在信誉和利润的驱动下,机构投资者也会存在羊群行为。大陆与台湾股市还有一个共同特点就是个人投资者多,而机构投资者少,因此,从对羊群行为的影响程度来说,个人投资者作用大于机构投资者。但不管怎么样,羊群行为对金融市场、甚至对经济稳定与增长的危害性都是巨大的。在股票市场未达到强效率之前,股票市场中羊群行为是不可避免的。但是,政府和监督机构可以努力采取一些措施减轻股票市场的羊群行为,为此,笔者建议:(一)强化信息的披露,提高信息的质量和投资者对信息的接受分析能力,减少投资的盲目性。(二)加强对机构投资者的监管,增加机构投资者的信息透明度,促使机构投资者树立正确的投资理念,提高金融市场的资本配置效率。(三)加强对投资者尤其是个人投资者的投资理论宣传和教育,提高股民的理论水平和对股票市场的理解,也是不可少的一项工作。(四)鼓励更多高水平的独立的中介机构从事评级、证券分析等业务以加强市场价格发现。

[参考文献]

[1] Kahneman 、Tversky,"Prospect Theory:An Analysis of Decision Making Under Risk"[J],《Econometra》1979,47:263 - 291

[2] Lakonishok J、Shleifer A、Vishny R,"Impact of Institutional Investors on Stock Prices"[J],《Journal of Financial Economics》,1992,32(1):23 - 43

[3] Chang E C、Cheng J W、Khorana A,"An examination of herd behavior in equity markets: An international perspective"[J],《Journal of Banking & Finance》,2000,24(10):1651 - 1679

[4] 孙培源、施东晖,"基于 CAPM 的中国股市羊群行为研究 —兼与宋军和吴冲锋先生商榷"[J],《经济研究》2002(2)

[5] 刘波、曾勇、唐小我,"中国股票市场羊群效应的实证研究"[J],《运筹与管理》2004(1)

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

查》指出,在规模较小的公司里,最重大的系统入侵案件有 32 %是内贼所为;在大企业中,因内部员工所为的重大系统入侵案件百分比更攀升到 48 %[3]。内部人员泄漏客户信息给信用卡用户造成重大损失。目前,中国信用卡市场仍属于开发阶段,信用卡信息安全事件在国内还没有发展到国外那种地步,不过,威胁信用卡安全的苗头在我国已经发生。据北京晚报报道,北京已经发生某银行职员向其它银行出售客户资料的事件,银行非网络信息安全正在引起政府和各相关部门的密切关注。信息安全是银行工作的重中之重。对于信息安全的管理,我国商业银行的现状是,工作重点放在对付外来黑客入侵的网络技术管理之上,而将内部员工的信息安全意识和安全教育放在次要的位置,对于防范内部人力资源的行为道德风险关注不多,内部控制存在一定程度的安全隐患。事实上,网络信息安全只是技术层面的问题,不管一项技术有多先进,也不过是辅助实现信息安全的手段而已,属于信息安全体系里的硬件部分,它还需要人和管理等软件的配合[4]。人的因素才是确保信息安全的关键因素。信息的安全需要建立在人员安全的基础之上。

二、ISO17799 标准及其人员安全性实施指南

1. ISO17799 的发展动态。ISO17799 是保护信息安全国际标准体系。它是根据英国标准协会(BSI)制定的信息安全标准 bs7799 修订而成。在信息安全的标准制订方面,英国最有成就。BS 7799 是目前国际上最知名的安全规范。英国标准协会于 1999 年 2 月提出了 BS 7799《信息安全管理体系标准》(The Code of Practice for Information Security),并于 1999 年 5 月进行了修订。1999 版包括 2 部分,《信息安全管理体系实施细则》(The code of practice for information security systems)和《信息安全管理体系规范》(Specification for Information Security Management Systems - ISMS)。2000 年 12 月国际标准化组织 ISO(The International Organization for Standardization)将 BS 7799 的第一部分正式转化成国际标准 ISO 17799。2002 年 9 月公布了 ISO17799 的第二部分,即 BS 7799 - 2;同年,还出版 ISO17799 工具箱[5]。ISO17799 采用管理和技术相结合的系统的方法,确定信息安全管理的方针和范围,在风险评估的基础上选择适宜的控制目标与控制方式来进行控制,制定业务持续性计划,建立并实施信息安全管理体系。它旨在帮助各种类型和规模的组织实施并运行有效的信息安全管理体系,从而增强企业识别、防止、减少和控制组织信息安全风险的能力。ISO17799 已同其它 ISO 国际标准一样成为金融、IT 企业、制造业、集团公司、上市公司和高新技术机构和政府部门提高管理水平的新体系。我国也已经开始将信息安全体系建设纳入到重要的议事日程,目前正在着手把国际信息安全管理标准 ISO17799 转化成国家标准,并即将进行首批国家信息安全标准认证单位资格审查和资格认证工作。

2. ISO17799 人员安全实施指南。ISO17799 标准的内容涉及 36 个管理目标和 127 个控制措施,全部内容分成 10 个领域。其中,针对人员管理部的部分主要体现在 10 个领域中的个人安全(Personnel Security)部分,概括起来包括以下三点[1]:

(1) 员工对信息安全的权利与义务。个人信息安全的权责应当在对员工聘用的阶段就开始实施,告知其工作的敏感性,并要求签订保密协议,并将员工所需担负的安全责任写入合约中,以便在以后员工的聘用期内时时进行监督。对处理敏感信息的员工进行相当程度的信用调查,必要时可定期进行或不定期的检查。若是经由第三者公司所委派,亦须遵循。人力资源风险管理是一个动态的过程,员工在不同的时间点都会有不同的个人情况,这些都会对他们的工作产生影响。不论个人情感或情绪或财务上的问题,行为或生活方式上的变化,都容易导致欺骗、偷窃、工作出错或其它安全上的问题。

(2) 对人员提供信息安全的教育培训。资产安全事件常常发生来自于使用者对资产安全的警觉性不佳及员工的无知,这就需要对员工进行信息安全教育培训。相关的第三用户也须如此。这样可以让员工定期了解环境的最新变化,这包括安全要求、法律责任和业务控制措施方面的内容,并在正常工作中切实遵守企业的安全政策,确保人员了解和识别信息安全存在的威胁和问题,尽可能地将安全风险降到最低。

(3) 建立安全事故和故障的处理及赏罚机制。信息安全事故的发生,包括破坏行为、威胁、弱点或故障,会影响企业资产的安全,所有人员、用户、第三者、承包商都应该了解并详实纪录,立即汇报。企业应建立一套完整的安全事件报告程序及一套安全事件的响应程序。所有人员、用户、第三者、承包商都应了解整个完整的程序。安全事件的响应程序对于重要的组件应有备援方案可供执行,以利紧急修复及故障排除。

鼓励员工要勇于面对问题,在发现或怀疑系统及服务有安全漏洞时,应立即通报,并着手处理,切勿因循苟且,把问题留给别人,并予以鼓励。相应地,对于违反企业安全政策及作业程序的雇员,应予以处罚,这对无视安全工作步骤的员工来,无疑是一种威慑。因此,企业内部应拟定奖励处罚的办法,即正式的惩戒规定,建立公正且正式的评议过程,并列入员工手册中。

三、ISO17799 对我国商业银行内部控制建设的启示与借鉴

1. 完善人事控管程序,重视操守,预先防范。员工的招聘和录用对银行业而言极为重要,尤其是当金融业招聘担任高风险的业务或工作时,更应该谨慎地控制招聘录用程序。

(1) 招聘。目前,我国的人才招聘多注重对应聘人员教育水平、工作经验、接受过的培训等能力进行鉴定,对他们的诚信和工作学习历史记录了解不多。这也是我国人力资源素质控制存在的问题。在条件允许的情况下,招聘单位必要时,可以考虑进行受聘者的家庭背景和以前的工作背景调查,特别是招聘担任财务、出纳或需接触金钱或有价证券之员工时,需要先经过信用背景调查,并提供保证人,如果保险公司开设了忠

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

诚险,可以考虑为该职务人员投保员工忠诚险。商业银行还应规定所有岗位的职责、权限和人员适任条件,明确关键岗位、特殊岗位、不相容岗位及其控制要求,对承办高风险业务之员工增加必要招聘控管程序,以降低日后的人为风险。除了招聘程序控管外,员工进入银行后,其职务可能会根据银行业务需要有所变动,当职务变动承担高风险工作内容时,银行高层主管需要再检查或验证员工之背景或信用调查,充分考虑人力资源管理过程中的风险。

(2)升迁。升迁是银行对员工工作表现之一种肯定,当银行提升某位员工至高层时,多数员工一定兴奋不已;当然也有员工认为其不胜任而拒绝升迁。对此种拒绝升迁情况,企业高层主管应与该员工面谈了解何种原因而不愿承接,同时亦可回头检查银行内部升迁程序是否有未考虑的地方,而需修正银行之升迁考核办法。或许可以透过与员工的再次面谈,发现任何异常表现,因而实时防止意外发生。

2. **推行 AB 角工作法,保证离职交接完整。**每个单位都会有人员新进、离职及调职等情况发生,当人员调职或离职,员工交接是极为重要的工作。尤其是确保员工交接工作完整,这又是一大议题。多数单位离职程序要经过层层部门之签证审核,例如:人事、总务等,但却往往不知如何确保交接完整。从内部控制考虑,最佳方式应该是重要职务工作平常就需有备援人员,也就是我国现在推广的 AB 角工作法,让同一职务至少有两位同仁清楚详细工作内容;另外,离职员工除了需完成离职程序外,最好能在主管签准离职时,列出交接清单并安排人员进行交接,并于该项工作交接清时,请离职员工及交接人员同时签字,以确保交接工作完整。

3. **加强银行保卫,监管人员进出。**加强银行保卫,监管人员进出,这道关卡的设计也叫存取控制(Access Control)。每天在有效时间内,规定每个员工的权限,并稽核员工进出纪录。同时,规定员工携带笔记型计算机进出银行办公场所都需经过一定程序的检查。

4. **培训员工,营造信息安全氛围。**商业银行应制定并保持培训计划,以确保高级管理层和全体员工能够完成其承担的内部控制方面的任务和职责。培训计划应定期评审,并应考虑不同层次员工的职责、能力和文化程度以及所面临的风险。另外,还可以通过讲座、研讨会、新闻媒体、网站和其它宣传方式将安全意识扩展为一种氛围,努力提高和强化社会的信息安全观念意识,确立信息安全管理的基本思想与政策,加快信息安全人才的培养,同时倡导信息伦理,提高公务员和公民的信息安全自律水平。这就将焦点从强制性的安全策略转换为自主接受的安全策略文化,这也是我们实现信息安全目标的基本前提[3]。

5. **培育企业文化,提高职业道德水平。**商业银行应培养健康的企业文化,对企业文化的内涵、组织机制、传播机制、评估机制以及奖罚机制做出明确的规定,向员工传达遵守法律法规和实施内部控制的重要性,引导员工树立良好的合规意识和较强的风险意识,促进员工职业道德水平的提高,规范员工行为,营造良好的内部控制环境。所有员工都应了解自己在内部控制中的作用,并鼓励员工批评、修改和完善银行内部控制,让员工全面参与内部控制体系建设。

四、结束语

目前,我国商业银行的信息安全工作走在所有行业的前头,但这并不意味着其他单位可以忽视信息安全。纵观企业的经营失败,有相当一部分企业是由于高级管理人员和掌握企业敏感信息内部人员背叛出卖企业机密信息的结果。在转轨经济信用缺失的今天,加强人员安全性控管显得特别重要。ISO17799 不外乎就是控管(Control)的观念,定义一套完整的政策、程序、实施与组织化的架构,用来提供合理的保障使企业目标得以达成,并避免、侦测或修正无法预期事件所造成的后果。因此,笔者建议在条件较为成熟的银行和企业应尽快试行 ISO17799,达到预先防治、应急处理及事后复原的基本要求,逐步形成广泛的安全文化和安全治理机制,建立与国际接轨的信息安全机制,拓展和完善我国企业内部控制机制。

[参考文献]

[1]ISO/IEC17799:2000,The code of practice for information security systems.

[2]邱海旭.800 万信用卡"偷窥"事件.2003 年 3 月 3 日.
http://finance.sina.com.cn/b/20030303/1518316297.shtml.

[3]庄强闵.企业内部人员的控管机制.2004 年 10 月 19 日.
http://www.ey.com/global/content.nsf/Taiwan/Issues&Perspectives-ISA-C.

[4]孙 强,郝亚斌.信息安全治理:创造新的战略竞争机遇.2004 年 4 月 7 日.
http://industry.ccidnet.com/pub/article/c35-a100965-p1.html.

[5]Jacquelin Bisson, René Saint - Germain. The BS 7799 / ISO 17799 Standard For a better approach to information security. 2004 年 10 月 19 日.
https://www.callio.com/bs7799/id,173。

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net