面向内部威胁的中观信息系统内部控制管理研究

刘国城[1],杨丽丽[2]

(1. 南京审计学院 金审学院,江苏 南京 211815;2. 安徽财经大学 工商管理学院,安徽 蚌埠 233041)

[摘 要]以"内部威胁"的防御为切入点,以"数据挖掘算法"为关键技术,以中观信息系统的审计决策与内控评价为研究目标,结合中观审计与信息系统审计的应用环境,构建"内部威胁"视角下"中观信息系统内控管理的模型",并在此基础上,力求建立适用于我国中观经济特色的信息系统内部控制管理体系。

[关键词]内部威胁;数据挖掘算法;内部控制;中观审计;内部审计;中观信息系统风险;信息系统审计

[中图分类号]F239.45 [文献标识码]A [文章编号]1004-4833(2014)06-0049-07

中观信息系统是指由两个或两个以上微观个体构成的中观主体所属的信息资源(如硬件、软件、传输设备、程序、数据以及经验),在整体核心控制台的统一控制下,以 Internet 为依托,按照一定的契约规则实施共享的网状结构式有机系统[1]。信息系统有宏观、中观与微观之分,宏观与中观信息系统特征相似。但与微观信息系统相比,中观信息系统功能更为复杂,主要体现为参与者之间在信息技术基础设施水平、信息化程度和能力上存在差异,参与者遵循一定的契约规则,依赖通信网络支持,对安全性的要求程度较高等。中观信息系统潜在威胁可以划分为内部威胁与外部威胁两类,本文仅研究中观信息系统内部威胁问题。内部威胁具有极强的隐蔽性与普遍性,中观信息系统只有加强对自身的内部控制管理,才能保证中观信息系统自身的保密性与实效性,促进中观信息系统自身功能的科学实现。为此,我国有必要尽快建立完善的中观信息系统内部控制管理体系,以便更好地监控中观信息系统的工作行为与运行机制,确保信息系统的良性运作。

一、相关理论概述与回顾

(一)内部威胁

"内部威胁"目前尚无权威的定义。Mcnamara 等学者认为,内部威胁是指对信息系统具有访问权限并且误用或滥用这些权限的人造成的威胁[2]。根据构造内部威胁模型所用到的系统特征来源,我们可以把现有的内部威胁模型分为主体模型和客体模型。主体模型以 Wood 提出的 CMO 模型[3]和 Parker 建立的 SKRAM 模型为代表[4],客体模型以 Park 等人提出的 CRBM 模型[5]和 Indrajit 等人提出的攻击树剪裁模型为代表[6]。其中 CMO 模型和 SKRAM 模型与传统的外部威胁解决方案明显不同,它们明确将信息系统中的主体对象作为建立内部威胁模型的主要数据来源,对相关信息进行分析以感知内部威胁。而 CRBM 模型和攻击树剪裁模型则借鉴了解决 outsider threat 的成熟技术,对信息系统中的客体对象进行了细致的分层量化。国内对于内部威胁的研究侧重两个方面:(1)基于"内部威胁"的概念特征、一般模型与防范策略进行基础理论研究。如赵战生等总结了内部威胁研究的起源和发展的历史阶段[7];兰昆等对内部威胁一般模型的建立方式进行了探索,对构成内部威胁攻击的

[收稿日期]2014-04-08

[基金项目]江苏高校哲学社会科学重点研究基地重大项目(2012JDXM010);教育部人文社会科学研究规划基金项目(14YJA790032);江苏省教育厅高校哲学社会科学研究基金(2012SJB630044)

[作者简介]刘国城(1978—),男,内蒙古赤峰人,南京审计学院金审学院副教授,从事信息系统审计理论研究;杨丽丽(1980—),女,河南焦作人,安徽财经大学工商管理学院讲师,从事内控管理研究。

必要因素进行了研究,描述了内部威胁攻击的综合模型[8];杨姗媛等提出了基于内部威胁的信息安全风险管理模型,从组织信息安全文化、奖惩等方面探索了防范信息系统内部威胁的措施[9]。我国学者对此方面的研究仅是针对不同视角提出各自在宏观层面的论点,还未形成有关内涵、动因、控制策略等由系列模块构成的深层次"内部威胁"有机理论体系。(2)对"内部威胁的一般模型"在某一特定视角下作拓展研究,构建全新的拓展模型。如崔鹏等在裁剪攻击树模型的基础上,提出基于用户操作树的内部威胁检测模型,该模型生成特定用户的操作树,通过分析用户操作树可以预测内部威胁的存在[10]。王辉等提出基于贝叶斯网络攻击图的内部威胁预测模型,描述内部攻击的路径与状态,计算内部威胁的危险概率[11]。国内学者在此方面已经积累了若干成果,但特定条件下众多拓展模型仅是理论上的假设与构思,至于在实践中适用程度如何,还需学者们长期的理论验证。纵观国内"内部威胁"研究的现状,未来学者的研究可由三个方向进行:首先,关注基本理论的纵深研究,而不应仅停留在框架与雏形阶段;其次,关注理论体系的有机构建,将零散的研究形式转向体系化形式;最后,拓展模型的构建需要结合实际问题,准确把握假设条件,以增强拓展模型的时效性与价值性。

(二)数据挖掘

数据挖掘的首次提出是在1995年加拿大蒙特利尔召开的首届KDD & Date Mining国际学术会议上。2000年第一次出版的《数据挖掘:概念与技术》一书深层次地提出了数据挖掘的理念、算法模型、数据维度建模的理论与方法[12]。20年来,国外对于数据挖掘理论的研究已经趋于成熟,并衍生出一系列数据挖掘算法,如决策树、贝叶斯网络、支持向量机、人工神经网络、频繁项集关联规则、K-means聚类等,这些算法的目标是挖掘隐藏在海量数据中新异的、有价值的、可解释的知识。与国外有关于"数据挖掘"的研究相比较,我国理论研究起步较晚。自1993年将数据挖掘引入国内以来,学界对数据挖掘的研究主要集中于两个方向:一是纵向延伸,即数据挖掘基本理论的纵深研究;二是横向应用,即数据挖掘算法与技术在银行、电信、保险、零售、医疗以及餐饮等商业领域的初步运用。多年来,国内将数据挖掘应用于信息系统"内部控制"的理论成果较少,不够深入且难成体系。如江伟等、黄力分析了异常检测算法在信息安全控制中的应用[13-14];张良等分析了决策树对信息安全审计策略的贡献[15];王会金通过设计挖掘流程,提出了适用于我国中观经济特色的信息系统审计风险控制框架[1];王红霞等探索了如何将多维数据聚类技术运用于电子政务审计分层抽样系统[16]。当然,研究体系的建立并非一蹴而就,且信息系统内部控制下数据挖掘算法的实施需满足特定假设条件(如内控数据质量的规范性),同时,数据挖掘算法自身具有特定的缺陷,如具体算法采用默认的参数设置并不总是最为合理,以致不能得到最佳的预测模型等。上述困难对如何将数据挖掘深入、系统地引入信息系统"控制"、"审计"与"管理"等问题的理论研究提出了全新的挑战。

二、内部威胁下中观信息系统风险的成因

近年来,内部威胁种类日益繁多,主要有四种表现形式:(1)电子设备使用方法不规范。如信息存储设备、个人数码助理等向信息系统引入病毒或植入间谍软件。(2)系统信息被泄露。通过电子邮件或百度Hi、YY语音、腾讯QQ、飞信等即时通讯方式将信息系统的运营数据以及客户数据不同程度地泄露。(3)台式电脑数据被偷窃,笔记本电脑与移动PC丢失所导致的丢失大量存储信息的威胁。(4)信息系统内部接触人员因缺乏教育或存在情绪因素,有意或无意地滥用信息系统,泄露系统内部重要信息[7]。中观信息系统风险是指成功利用中观信息系统的脆弱性或漏洞,造成系统损害的可能性,当任何一类内部威胁作用于中观信息系统的脆弱点或漏洞点时,都可能会产生中观信息系统潜在风险。

中观信息系统风险的成因有很多种,本文只分析面向内部威胁的中观信息系统风险成因。下页图1显示了内部威胁、内部控制与中观信息系统风险三者的作用关系,以及中观信息系统风险自身的构成。对于中观信息系统而言,其内部威胁的主体包括本企业员工、合同工、顾问、临时员工、以前在

该组织供职的人员，甚至包括第三方商业伙伴。内部威胁的产生源自两个方面：(1)信息系统内部人员对资源的滥用和误用；(2)系统中资源本身缺乏充足的安全保障措施，容易被内部人员利用，从而造成系统的危害。内部威胁的主要特点是：(1)内部人员具有合法身份，拥有访问系统资源的权限，常规的系统安全保护措施和防御体系(如身份认证，防火墙等)对内部人员不起作用；(2)内部人员非常熟悉系统的内部结构、运作方式、相关文化，这使得他们的行动非常隐蔽，难以被发现；(3)内部人员最容易接触敏感信息，行动非常有针对性。因而，此类危害往往针对系统中最核心、最珍贵的资源。

内部威胁并不能直接产生中观信息系统风险，这主要看内部威胁与中观信息系统风险之间的作用机理(见图1)：第一步，内部威胁首先作用于中观信息系统的脆弱点，即在系统安全程序、管理控制、物理设计中存在的、可能被攻击者用来获得未授权信息或破坏关键处理的弱点[17]，主要居于物理环境、技术环境、管理环境与法律环境之中。当内部威胁作用于上述脆弱点后，才可能产生中观信息系统风险，但不绝对。第二步，针对中观信息系统脆弱点，要看中观信息系统是否有相应完善、科学的内部控制制度。第三步，如果第二步骤发现中观信息系统并未建立完备有效的内部控制制度，作用于脆弱点的内部威胁将会造成中观信息系统损失，由此必会形成中观信息系统风险。第四步，如果第二步骤发现中观信息系统已经建立完备有效的内部控制制度，也可能会出现中观信息系统风险，但不绝对。第五步，如果第四步骤已经形成了科学的内部控制制度，但内部控制制度的执行缺乏有效性，内部控制制度流于形式，此时作用于脆弱点的内部威胁也将会造成中观信息系统损失，从而产生中观信息系统风险。第六步，如果第四步骤已经形成了科学的内部控制制度，且既定内部控制制度的执行合理有效，此时，内部控制这一“天然屏障”的存在使得内部威胁被“有效屏蔽”，中观信息系统风险绝对不会出现。从上述步骤可见，当内部威胁作用于中观信息系统脆弱点时，内部控制制度设计失效以及执行失效都将会导致中观信息系统风险的产生。鉴于此，若要有效抵御中观信息系统因内部威胁而产生的风险，就必须要对中观信息系统内部控制实施有效管理。

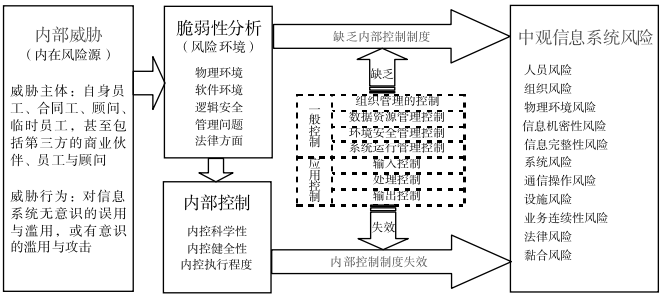

图1　内部威胁与中观信息系统风险的作用机制

三、数据挖掘算法对内部威胁下中观信息系统内部控制管理的贡献

中观信息系统内部控制管理是指中观经济主体运用科学系统的程序方法，对中观经济主体信息系统的控制规程与控制政策所实施的一种管理活动，该活动蕴含内控制度设计、内控制度测试、内控制度评价以及内部审计建议等行为，旨在增强中观经济主体特定信息网络的有效性、安全性、机密性与一致性，以确保中观信息系统自身功能的高效实现。内部用户给信息系统带来的内部威胁远大于技术非凡的网络黑客所带来的外在威胁，同时也更为隐蔽，因而，面向内部威胁的中观信息系统内部控制管理难度更大，过程更为复杂。本文认为，数据挖掘的算法和流程通过采用定量的、工程性的方法研究内部控制管理，将会使原来模糊的控制制度变得更为清晰并可准确度量。

(一) 数据挖掘算法与中观信息系统内部控制的契合分析

中观信息系统在运行中会产生大量的数据，不同行业的信息系统数据有不同的特点。例如，北京市东城区社区卫生系统是一个基于联机事务处理的医院信息系统，该中观信息系统的数据源主要包含医疗业务数据、医药药品与医疗设备物流数据、行政后勤数据以及存放于系统日志的信息系统构建与运营的所有数据。面对大规模的诊断业务，众多医务与行政等内部用户在社区卫生系统中建立了海量的数据。这些数据可能是重复或不完整的，也可能是敏感或可疑的，还可能是噪声数据，然而在

海量数据中,我们总能发现某些数据的共同属性及某类数据的共同价值。数据挖掘是从海量数据中挖掘有用的信息,即从大量的、不完全的、有噪声的、随机的实际应用数据中发现隐含的、规律性的、人们事先未知的,但又是潜在有用的并且最终可理解的信息和知识的非平凡过程[18]。上述医院信息系统在运行中所提供的海量数据以及散布的众多特征,为信息系统内部控制管理实施数据挖掘行为提供了必要前提。如果数据匮乏,数据无法聚类,则数据挖掘行为将无法开展。而中观信息系统内部控制管理所获取的数据则完全具备数据挖掘的前提假设。

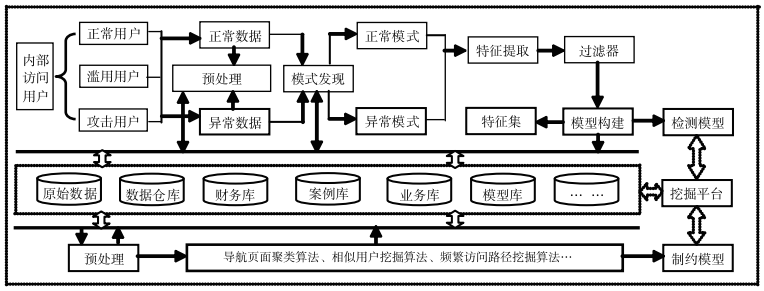

图 2　数据挖掘在内部威胁下中观信息系统内部控制管理中的规划思路

当然,内部威胁下的中观信息系统内部控制管理过程需要数据挖掘算法,这是因为信息系统内部控制制度中所包含的具体条款中,绝大部分是由“内部控制人员”或“内部审计人员”根据个人知识制定的,制度制定者并非“完全理性的经济人”,他们只具备有限的决策能力与选择能力,这种定性研究方法下的经验判断难免会带有一定的主观性,缺乏科学性。将数据挖掘原理与算法引入中观信息系统内部控制管理过程,不但可行,而且是一种创新。例如,系统内部控制制度中的某项条款是“内部用户访问系统和服务的权限必须通过授权,用户名必须为英文字母全拼,初始密码为‘身份证后六位 + 工号’,初次进入后必须自行修改密码,且位数≥12”。我们仅选取授权用户的英文字母全拼作为“特征字段”,通过对某一范围内授权用户初次登录的日志数据实施挖掘流程,结果发现:(1)授权用户若使用其他授权用户的初始密码同样可以访问该系统;(2)授权用户若使用大写英文字母作为用户名,尽管登录密码正确,也无法访问该系统。因而,通过挖掘,我们应在内控条款里加入“小写英文”的字样,同时应该重新修正登录系统的应用程序,实现“一对一”访问。数据挖掘算法主要运用的是数学方法,实现了研究方法由定性形式向定量形式的转化,进而弥补了中观信息系统在内部控制管理思路设计上的主观判断,能够使信息系统内部控制制度得到有效的纠正与科学的补充。

(二) 中观信息系统内部控制管理过程中数据挖掘流程的应用

内部威胁下中观信息系统内部控制管理过程中的挖掘流程相对复杂(见图 2),可归纳为以下步骤。(1)数据预处理。内部访问用户包括正常用户、滥用用户与攻击用户三类,他们在访问信息系统时留下了正常数据与异常数据。尽管这些数据是原始的或粗糙的,但形成了由原始数据、Web 访问记录与日志文件等组成的目标数据集,为保证数据挖掘行为的有效运作,这些数据必须经过事先处理,即预处理。数据的预处理包含数据选取过程、数据表属性一致化过程、数据清理过程以及数据归约过程。数据归约过程是数据形式变换过程与数据压缩过程,其对挖掘的后续工作至关重要。(2)模式发现。模式发现是指通过观测与预测,去寻找与揭示事物规则与本质的过程。本步骤的模式发现是对上一步骤所产生的清洗数据及转换数据,通过分类与聚类等技术,从样本数据中找出规律,有效辨别正常模式与异常模式。(3)模型构建。本步骤是利用前两步骤已有的知识,在对已生成的数据进行特征提取并进一步过滤的基础上,将一般规律与普遍情况抽象成一种分析模型。该模型是某个数据子集的形式化描述。当然,所构建的模型可采取不同的形式,具体采用何种形式关键要看“模式发现”过程所观测的数据特征。基于内部访问用户的日志数据属性来看,剪枝算法、相似用户挖掘算法、频繁访问路径挖掘算法以及离群数据点算法更适用于中观信息系统内部控制管理的知识发现。(4)模型评估。本步骤是对挖掘结果进行验证与评价。有时通过数据挖掘所得到的结论可能是没有

实际价值的，也许不能全面反映某类数据的真正内涵。因此，在本步骤必须采用未来数据对模型重新验证，识别挖掘过程是否存在偏差，哪些细节偏离决策需求。（5）知识发现。本步骤是实现数据挖掘目标的过程，通过语言或图形等方式将抽象的数据挖掘结论描述与归纳成易于掌握的知识。上述中第三步骤是整个数据挖掘过程成功的关键。例如，针对供应链金融信息系统的内部控制管理，关于如何完成“模型构建”，需要依次遵循以下路线：①对各类内部访问用户进行系统元操作，生成用户元操作组合；②借助剪枝算法对用户元操作组合生成用户剪枝子树；③运用最小攻击树算法进一步将剪枝子树生成用户最小攻击树；④有针对性地通过前述的用户最小攻击树检测供应链金融信息系统业务运营、日志处理等预处理信息及其模式发现，若“树为空”，则为“正常用户”，若“树非空”，则为“威胁用户”；⑤忽略“正常用户”，仅针对“威胁用户”确定“极限阀值 R”，运用攻击检测算法生成“威胁用户攻击进度 Y”，若“Y < R”，则为“可疑用户”，若“Y > R”，则为“恶意用户”；⑥对“恶意用户”中断操作，对“可疑用户”实时监控。如上页图 2 所示，①—⑤步骤的实施过程是在一个特定的数据挖掘平台（M 平台）实现的，M 平台由数据仓库、案例库、业务库、模型库等系列“库”搭建而成，是数据清洗、提炼、挖掘，规律发现、知识总结的操作台。通过 M 平台，大量的内部威胁数据将被筛选，防范内部威胁的中观信息系统内部控制制度将得到更深层次的完善与优化。

四、面向内部威胁的中观信息系统内部控制管理体系的构建

中观信息系统内部控制管理体系的构建是一个复杂的过程，下面阐述如何建立该体系（见图 3）。

（一）第一层次：初步构架内部威胁下的中观信息系统内部控制框架

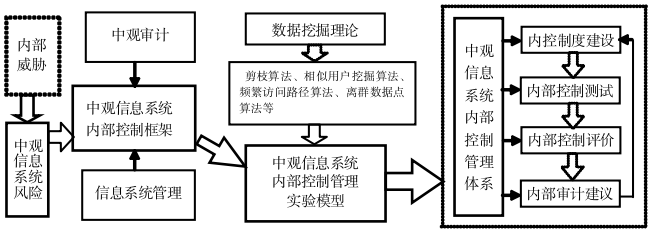

图 3　面向内部威胁的中观信息系统内部控制管理体系

中观信息系统的内部威胁主要来自于系统自身软硬件维护与支持人员、访问信息系统或共享数据库的商业伙伴、清洁工以及保安等支持服务人员、临时员工、顾问等主体，这些主体对信息系统的访问有临时访问与常驻访问两种形式。鉴于内部访问主体的特征与访问形式的特点，中观经济主体需要以中观审计理论与信息系统管理理论为依据，从信息系统的“一般控制”与“应用控制”两个方面构建针对内部访问威胁的内部控制框架。在“一般控制”方面，内部控制框架至少涵盖四项内容：（1）“组织控制”的一般原则与具体措施；（2）“数据资源管理控制”的一般原则与具体措施；（3）“环境安全管理控制”的一般原则与具体措施；（4）“系统运行管理控制”的一般原则与具体措施。例如，在“组织控制”内容上，中观经济主体应该为不同角色员工制定一个描述他们正常任务和职责的工作说明，工作说明包括实施方针的通用职责和保护具体资产、执行具体安全程序或活动的职责。这个工作说明既要包含岗位职责，也要包含执行具体活动的相关程序。在“环境安全管理控制”内容上，中观经济主体应该制定一系列系统设备维护的原则与规范，规范应包含“只有经过授权的维护人员才能维修和保养设备”、“维修人员应具有一定的相关维修技能”、“应保持所有有疑问或实际缺陷以及所有预防和纠正措施的记录”等关键要素，仅有如此，系统才能保持持续的可用性与完整性。在“应用控制”方面，内部控制框架至少包括三项内容：（1）“输入控制”的关键要素与相应策略；（2）“处理控制”的关键要素与相应策略；（3）“输出控制”的关键要素与相应策略。例如，在“输入控制”方面，有必要事先规定数据的输入格式，编制数据输入工作的方法与程序，有效确立数据在传送、输入过程中对所出现的错误进行记录的机制，规定数据输入过程中所涉及全部人员的责任。又如，在“输出控制”方面，信息系统数据的输出，无论是磁盘介质还是纸质资料，相关内部人员都要做到绝对保密。因此，对于参与信息输出的内部人员，中观经济主体应该与其签署保密

协议,明确其工作职责与义务,建立相应的约束与规范,以防止输出数据的泄露与篡改。

(二)第二层次:引入数据挖掘算法验证中观信息系统内部控制管理的实验模型

第一层次所构架的内部控制框架是中观经济主体根据自身经验以及模仿外来知识所建立的一个内部控制初始框架。这个框架仅是一个雏形,可能不够具体,较为粗糙,部分控制原则与控制策略也可能不够科学,某些控制思路可能不够符合中观信息系统自身的特点,存在片面性。第二层次是对第一层次相关控制思路、原则与策略的验证、校正与优化。为了更好地实现对第一层次即内部控制框架雏形的验证与校正功能,在第二层次的研究中,需要借助前文所述的数据挖掘算法。第二层次的实施主要包含以下过程。(1)基于中观信息系统自身所积累的数据建立适用于一般数据挖掘算法的主题数据库;(2)在主题数据库下,利用数据挖掘理论中的剪枝算法、相似用户挖掘算法、频繁访问路径算法、离群数据点算法等,对第一层次所设计的框架雏形构建具体的控制模型,按照相应的控制属性进行控制测试。如控制聚类时,可采用系统聚类法,它能够生成层次化的嵌套簇,且准确度较高。对于矩阵 Aa * b 的行向量 A(i, *),系统聚类法的具体过程有:①将 Aa * b 中的每个行向量 A(i, *)视为一个具有单个成员的簇 ni = A(i, *),这些簇构成了 Aa * b 的一个聚类 N = {n1,…,ni,…,na};②计算 N 中每对簇(ni,np)之间的相似度 Sim(ni,np),其中 1≤i,p≤a,i≠p;③选取具有最大相似度的簇对 argmaxsim(ni,np),并将 ni 和 np 合并为一个新簇 nk = ni∪np,从而构成了 Aa * b 的一个新的聚类 N = {n1,…,nk,…,na - 1};④重复上述步骤,直至 N 中剩下一个簇为止;⑤由以上过程构造出一棵聚类树,其中包含簇的层次信息与所有簇内和簇间的相似度;⑥决定类的个数和类项;(3)对上述挖掘模型进行结论分析与验证评价。

(三)第三层次:建立全面的中观信息系统内部控制管理体系

第三层次是第一层次与第二层次的提炼过程,也是中观信息系统内部控制管理体系的凝练过程。第三层次所建立的中观信息系统内部控制管理体系由四个部分构成,四部分之间的逻辑关系见上页图 3,每部分表述具体如下。(1)内控制度建设。这一部分的主要作用是初次建立或补充原有关于中观信息系统内部控制的各项规范、措施与制度。例如,以往中观经济主体与所有员工并未商定过信息保密的契约,但由于总是存在员工泄露组织机密的风险,因而在这一部分,中观经济主体应该建立与相关员工签订保密协议的制度,并将其作为雇用合同基本条款和条件的一部分。(2)内部控制测试。这一部分是对第一部分所提出的中观信息系统内控制度的整体性、实效性以及适应性等方面实施控制测试。此部分的内部控制测试只需关注两个方向,一是既有信息系统内部控制制度设计上的科学性与健全性,二是既有内部控制制度执行上的有效性与时效性。在上述科学性、健全性、有效性以及时效性的测试方面,更多采用的是检查、观察、询问、重新计算、重新复核、重新分析等审计一般方法与技术,此外还需要引入“外脑”,即数据挖掘具体算法,这样,内控制度的测试才更具科学性与准确性。(3)内部控制评价。这一部分是针对第二部分而言的,主要是对第二部分所产生的测试数据等证据进行分析,基于第二部分的取证证据,最终评估并判断第一部分由个人认识和主观经验而形成不够完备的内部控制制度在设计上是否科学、全面,执行上是否有效、持续。(4)内部审计建议。这一部分是针对体系中第三部分而言的,主要是对第三部分所发现的问题进行修正、补充、改进。例如,有一关于“文件控制”的条款是“文件标明初建日期,每次修订标明日期,分开归类保存”,但该条款通过测试后的评价为“每次修订的文件将覆盖原文件,修订日期混淆为文件初建日期”,这类问题属于执行上的问题,因而应该加强执行方面的建议措施与奖惩力度。体系的四个部分相辅相成,彼此衔接,第四部分又为第一部分提供了全新的补充。

五、结束语

本文运用数据挖掘算法构建了面向内部威胁的中观信息系统内部控制管理体系,为中观经济主体如何管理网状信息系统提供指导与借鉴。需要指出的是,在构建中观信息系统内部控制管理体系

的过程中,科学引入数据挖掘算法是一个复杂的过程,涉及数据仓库建立、挖掘算法遴选、在线分析处理等多个层面。本文将数据挖掘算法引入内部威胁下中观信息系统内部控制管理体系的构建,本身是一种尝试,提出的是相对宏观的设计思路。这种尝试是有价值的,它使信息系统内部控制方面的理论研究由定性转向了定量。然而,在研究中,还要关注将数据挖掘算法应用于信息系统内部控制滋生的局限性,如何化解上述矛盾,还亟待更为深入地探索。

参考文献:

[1]王会金. 中观信息系统审计风险控制体系研究——以 COBIT 框架与数据挖掘技术相结合为视角[J]. 审计与经济研究,2012(1):16-23.

[2]McKenna R. Danger of the insider threat[J]. Infosecurity,2007(2):5-15.

[3]Wood B J. An insider threat model for adversary siumlation[C]. Proceedings of a workshop with title "Research on Mitigating the Insider Threat to Information Systems". Arlington VA,2000.

[4]Parker D B. Fighting computer crime: a nes framework for protecting information[M]. New York: John Wiley & Sons,1998.

[5]Park J S, Ho S M. Composite role-based monitoring (CRBM) for countering insider threats[C]. Proceedings of the Intelligence and Security Informatics, USA,2004.

[6]Indrajit R, Poolsapassit N. Useing attack trees to identify malicious attacks from authorized insiders[J]. Proceedings of the Computer Security—ESORICS,2005,38(1):231-246.

[7]赵战生,左晓栋."攘外"勿忘"安内"——谈 insider 威胁研究[J]. 网络安全技术与应用,2001(9):10-15.

[8]兰昆,方勇. 网络信息系统的内部威胁模型研究[J]. 计算机工程与应用,2004(11):129-131.

[9]杨姗媛,朱建明. 基于内部威胁的信息安全风险管理模型及防范措施[J]. 管理现代化,2013(2):47-49.

[10]崔鹏,姚丹霖. 基于用户操作树的内部威胁检测模型[J]. 河北省科学院学报,2008(1):10-14.

[11]王辉,杨光灿,韩冬梅. 基于贝叶斯网络的内部威胁预测研究[J]. 计算机应用研究,2013(9):68-71.

[12]Han Jiawei, Kamber M. 数据挖掘:概念与技术[M]. 3 版. 北京:机械工业出版社,2012.

[13]江伟,陈龙,王国胤. 用户行为异常检测在安全审计系统中的应用[J]. 计算机应用,2006(7):37-42.

[14]黄力. 数据挖掘理论在安全审计分析中的应用[J]. 微计算机信息,2007(9):147-149.

[15]张良,何华. 基于决策树的安全审计策略自适应管理控制平台[J]. 科技导报,2010(12):67-70.

[16]王红霞,景波. 多维数据聚类技术在电子政务审计分层抽样中的引用研究[J]. 商业会计,2014(1):69-71.

[17]刘国城,王会金. BS7799 标准及其在中观信息系统审计中的应用[J]. 审计与经济研究,2012(3):50-56.

[18]张云涛,龚玲. 数据挖掘原理与技术[M]. 北京:电子工业出版社,2004.

[责任编辑:高　婷]

Internal Control Management of Meso-information Systems Coping with Insider Threat

LIU Guocheng[1], YANG Lili[2]

(1. Nanjing Audit University, Nanjing 211815, China;
2. Anhui University of Finance and Economics, Bengbu 233041, China)

Abstract: In this paper, it takes the defense of "insider threat" as an entry point, the "data mining algorithms" as the key technology, the audit decision-making and evaluation of internal control of meso-information system as the research objective, in combination with the application environment of meso-audit and information system audit, the model of internal control management of meso-information system is constructed under the perspective of "insider threat", based on which, the internal control management of information system suitable for Chinese meso-economy is to be established.

Key Words: insider threat; data mining algorithms; meso-audit; internal control; meso-information system risk; information system audit