文章编号:2095-0365(2011)02-0040-05

信息安全外包风险识别与评估模型研究

梁志顺

(张家口市交通局,河北 张家口 075000)

摘 要:针对信息安全外包的业务流程,运用系统理论分析,识别外包服务的关键风险因素,提出基于第三方认证的风险评估框架,构建了评估指标体系,结合我国风险管理政策制定安全服务商服务风险监测规则,更好管理外包风险。

关键词:信息安全外包;风险管理;风险评估

中图分类号:F270 文献标识码:A

企业为了消除安全困扰,一方面加大对IT员工以及企业自身的安全培训,更多的企业通过寻找托管信息安全管理服务提供商(MSSP)来进行实时或定期的安全服务。信息安全外包服务是以第三方的服务来完成企业内部的信息系统相关工作的一种全方位、系统的安全服务。[1]市场调查公司Yankee Group表示,到2010年,美国将有90%的企业安全通过外包来实现。[2]国内近些年出现一些安全服务外包商,但提供的产品和服务质量良莠不齐,行业内尚未发展成一致的参考模型和评价标准,相关的法律法规不健全,不能有效地管理企业和安全服务外包方的契约关系,外包维护管理质量处于失控状态,安全外包的预期差强人意。[3]外包服务的风险管理与可信评估成为企业是否选择外包的关键。

一、外包风险成因

信息安全外包风险可以定义为一切扰乱外包服务运作的威胁。[4]因为企业与服务商的协调、合作中存在着各种不确定性,有不确定性就有风险存在。信息安全外包风险评估的目的是在信息不对称的情况下最大可能控制外包风险。

图1的外包流程显示:企业有了安全需求,需要寻找服务商,服务商构建了解决方案,通过向企业提供服务获利。该流程中,主动参与的实体有服务商和企业,被动实体有解决方案、安全产品和各种服务(安全服务商所能提供的服务包括:网络入侵监测以及防护,主机入侵防护,系统漏洞评估,补丁管理,防火墙和VPN管理,针对病毒和垃圾邮件的电子邮件监控等)。[2]

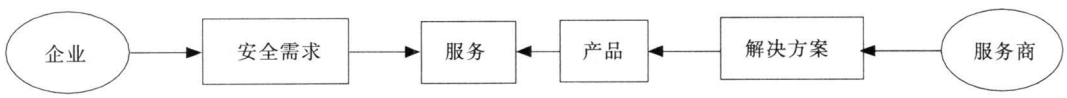

图1 外包服务流程

运用系统理论研究,可以发现如下问题:

(1)流程中缺乏对外包商的服务行为监督。

(2)缺乏双向沟通机制。外包服务过程是一个动态的螺旋上升的过程。随着企业环境和对安全级别要求的改变,外包服务需要也处于变动之中,必须通过双方的沟通,处理好各种变化,降低过程中产生的不确定。

(3)缺乏风险释放机制。整个过程的风险无法定量估计,导致风险逐渐积累,一旦意识到风险,已经无法避免。

(4)缺乏第三方的认证。服务商的资质与服务信誉成正比,如果有可信的资质认证,可以增加

收稿日期:2011-03-29

作者简介:梁志顺(1972-),男,工程师,研究方向:工程管理。

企业的信心。

二、外包风险识别

ELF Atochem 公司的副总裁和 CIO Robert Rubin 指出, 外包中存在大量的不确定性因素, 必须进行管理。如果不对外包进行适当的管理, 公司的信息流将处于巨大的风险之中。[3]

(一) 信息安全外包的规划与战略风险

这类风险体现在如下几个方面: 一是某些企业没有上升到企业战略的层面考虑信息化问题, 仅从降低成本的角度来处理信息安全外包问题; 二是有些企业并未透彻地分析自己的信息安全需求, 更谈不上进行科学合理的信息安全资源规划; 三是对信息安全外包的认识模糊, 没有真正理解信息安全外包服务的具体内容、分类、操作流程以及对企业的意义和作用。

(二) 信息服务提供商选择风险

目前信息安全外包市场缺乏主导厂商, 提供低端服务的小公司较多, 且其提供的服务质量参差不齐。各厂商往往打出各种“ 技术牌、概念牌、成功案例牌”, 令企业眼花缭乱、真伪难辨。如果遇到服务提供商倒闭, 后果更是不堪设想。[4] 企业在评估和选择信息外包服务方面没有成熟的方法, 难以做出正确的抉择。

(三) 契约风险

信息安全外包服务合同缺乏可供借鉴的经验, 往往依据外包服务提供商提供的所谓“ 标准”合同, 不加改动就签署。[5] 而这类标准合同中往往包含着大量令非专业人士无法理解的技术指标和专业名词, 这些指标和名词本身并不等价于企业所需要的安全服务, 可是背后却常常隐藏着额外的费用。另一方面, 由于外包合同在大多数的情况下是不完善的, 合同逐步实施的同时环境也是不断变化的, 所以在合同中不可能对外包服务需求的所有环节都做出具体的规定。

(四) 失控风险

这类风险包括三个方面: 一是企业缺乏对信息安全外包服务质量的控制方法, 对提供服务是否达到契约标准无法做出及时的识别和有效的证明; 二是企业丧失成本控制能力, 服务商以各种理由诱导企业, 将项目越做越多, 越做越大, 成本不断增加; 三是企业丧失外包过程中形成的知识产权的所有权。

(五) 企业内部变革的风险

企业要实施安全外包必然涉及到其内部相关部门的变革, 以配合外包商共同完成对企业信息安全的管理与控制, 而变革又往往伴随着利益的冲突和再分配。因此, 信息中心负责人的思想观念, 信息中心职能的转变不及时、不到位, 原信息中心员工的安置不妥都会对信息安全外包的实施造成巨大影响。

(六) 信息泄漏风险

实施安全外包, 外包商不可避免会接触到企业的内部信息。而企业信息往往涉及商业秘密。其中客户资源信息和企业战略机密等重要信息最易泄漏。因为企业仅仅从技术上对外包商进行了考量, 至于品质还需要用契约去规范。

(七) 丧失灵活性和对服务提供商依赖性的风险

企业把信息安全外包出去最大的风险在于失去控制权和可视性, 并对外包商产生很高的依赖性。安全外包就是一把双刃剑, 在降低成本同时也承担风险。

三、风险评估框架

(一) 可信评估需求

1. 高层安全需求

服务外包商在服务的交付过程中, 应当保证企业资产的机密性、可用性和完整性, 并使企业满意。企业需要保密的东西包括但不仅限于已经标识出来的数据、安全性、脆弱性和受到攻击的状态。服务外包商应保证企业的特定数据仅可在企业所在的国家使用以满足区域性的数据保密法规。

2. 服务可用性需求

企业所需要的服务可用性的时间和其他限制, 根据经验来确定对服务可用性的要求。服务的可用性的预留时间已经包括了部门协调的预留时间、软硬件和数据的维护升级而预定的停机时间。服务可用性的另外一方面的内容, 是说明服务故障或不可用时的反应时间。

3. 契约需求

在确定了企业服务需求之后,应该定义契约结构,包括服务的实现,服务的期限,服务设备的安全性以及安装方面的注意事项等。

4. 服务可增容性的需求

企业将协同服务外包商搜集关于服务容量的数据,例如服务宽度和正在使用的服务系统的能力百分率等。企业需要详细说明其对能力增长、存储需求、周期性或奖励性机制的预期率。外包商则需要向企业说明所有服务可用性和生产定额的增长可能引发的预期影响。双方经过协商,决定在这个部分中服务增容的限度,方式,解决所涉及的机构等方面的问题。

5. 双向沟通需求

协议中需要规定服务中沟通的方式和种类,如外包商呈交给企业的报告的种类和形式。服务控制中应该规定双方共同商定的报告样本。报告的种类至少应该包括:服务水平报告,提供外包商服务水平和最低服务水平的比较;违章报告:已经出现或可能出现的违章登陆和访问;事件报告:已出现或可能实现的入侵事件。

(二)风险评估框架

参考国际标准ISO/IEC 17799:2000《信息技术—信息安全管理实施规则》;ISO/IEC 27001:2005《信息安全管理体系规范》和国家标准GB/T 18336-2001《信息技术安全性评估准则》制定风险评估框架。框架如图2所示。框架的基本思想为:从风险控制目标出发,从实现信息安全外包过程的三个层面,按照风险等级的不同要求,对外包过程进行控制和管理,实现对不同风险进行分等级保护。

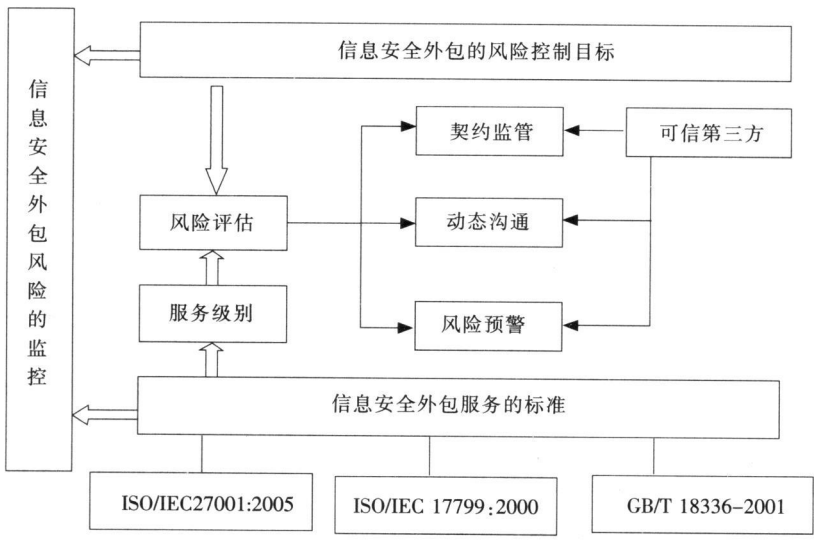

图2 风险评估框架

1. 风险等级

根据国家标准GB/T20269—20273中的服务标准,信息安全等级分为D类(没有任何保护的)、C类(分为C1和C2级)、B类(分为B1、B2、B3)、A类和超A类,共五级,与此相对应,风险也可以分为五级,依据用户的行为得分划分。[6]

2. 服务级别管理

安全外包服务的控制实施要通过服务级别来管理。服务级别管理包括定义、匹配、存档和管理客户要求的各个级别的服务。这些服务级别受到服务成本的约束。服务级别管理包括制订服务级别协议。服务级别协议包括服务分类和回顾会等内容。

3. 服务的监督和控制

监督是用来观察外包商是否在做他应该做的事情。如果通过监督发现外包商正在偏离预定的行为目标,此时就需要控制,控制就是使外包商返回到正确的轨道上去。在有了控制规则来规范外包商服务绩效之后,要保持外包商和企业客户经常的沟通,以便能够及时发现问题,进行标准化的控制活动。

4. 第三方认证

2003年中央颁布《国家信息化灵动小组关于加强信息安全保障工作的意见》,提出建立信息安全认证认可体系的要求,2007年国家网络与信息协调小组着手建立信息安全服务资质认证认可制

度。为体现认证、认可制度的公平、公开、公正, 须由可信第三方对信息安全服务组织的“服务能力”进行全面、综合、客观地评价。因此, 除了企业和外包商严格按照契约所规定的权责管理外包服务, 与此同时, 还应有第三方的认证管理。从更高的程度上约束双方的权利和义务, 为外包服务的有力实施提供了准则和保障。

四、风险评估实施

(一) 风险评估周期

风险评估应该划定评估周期, 如: 一年可以划定 2 个评估期, 4 月至 9 月为一个评估期, 10 月至次年 3 月为一个评价期。评估结果分为非常满意、满意、不满意三个等级, 依据各服务项目扣分情况确定等级。

(二) 服务商行为认定

安全服务商在招投标、合同的签订和履行以及售后服务过程中发生的, 有关违反法律、法规、规章和有关规定的行为, 按照其行为的不利影响程度, 分为一般行为、不良行为和严重不良行为三类[7]。如表 1 所示。其中不良行为和严重不良行为是指服务商在招投标、合同的签订和履行过程中发生的, 违反有关法律、法规和规章的, 或是严重损害使用方利益的行为。

1. 严重不良行为认定

以各种方式弄虚作假, 骗取中标; 相互串通投标报价; 因供应商原因未按需求计划及时交货, 经两次催告, 在合理时间内仍不交货; 因产品质量问题造成安全信息泄露和业务系统中断事故; 其它契约规定的严重不良行为。

2. 不良行为认定

服务商在竞标结束未及时签订合同, 经三次催告后, 在合理时间内仍不签订合同; 转包或违法分包中标产品或服务; 服务过程中, 未及时提供产品合格证书、检验证书、说明书、提货单和监造证明, 经三次催告, 除特殊情况外, 在合理时间内仍不提供服务报告及问题说明的。

(三) 风险评估指标

不良行为是根据本行业和其他行业知识的预先定义, 服务中还会出现各种各样的问题, 应该从服务商的服务历史中逐步挖掘行为模式, 如表 1。添加到已经定义的行为模式库中, 加强风险的管理与控制。

表 **1**　服务商行为评估指标

一级指标	二级指标
投标与签约情况	是否要求撤销其投标文件
	是否按规定时间签约
	是否按规定提供履约保证金
履约情况	产品资料齐全情况
	按时服务情况
	服务质量情况
	紧急服务情况

参考文献:

[1] 陈晓桦, 翟亚红. 关于我国开展信息安全服务资质认证工作的思考[J]. 信息安全与通信保密, 2007(10): 19-21.

[2] mike. 如何外包安全管理项目[EB/OL]. http://www.csai.cn.2008-05.

[3] 戴译. 如何选择远程通信服务商[EB/OL]. 2008. http://www2.ccw.com.cn/1998/13/166624.shtml. 2008-06.

[4] 张勇谦. 网络安全外包服务市场分析[D]. 北京: 北京邮电大学, 2007.

[5] 胡克瑾. 信息安全外包的控制与管理框架的研究[D]. 上海: 同济大学, 2006.

[6] 陆宝华. 等级保护概述——著名等级保护专家陆宝华谈我国信息安全等级保护概况[EB/OL]. http://www.sinoit.org.cn/NewsLetter/NO.3/20090101.html. 2008-08.

[7] 中国国家标准局. 企业信用评价指标体系分类及代码规范[DB/OL]. http://www.xybz.org/news/20081091130191 61.htm. 2008-11-01.

(下转第 95 页)

impact on their living conditions, developing state and interest claim. In this paper, we conduct a questionnaire survey among young teachers in Tianjin city. Based on Factor Analysis findings, seven influence factors are summarized and analyzed to provide basis for sustainable development of young teachers in college.

Key words: young teachers in college; questionnaire survey; factor analysis

(上接第 43 页)

Research On Risk Identification and Assessment Model for Information Security Outsourcing

LIANG Zhi-shun

(Transportation Department of Zhangjiakou 075000, China)

Abstract: The thesis aims at the information security outsourcing risk identification and assessment. First, an analysis is made of the deficiency of work flow through system theory , then the key risk factors of outsourcing are identified, and the frame of risk assessment is set up based on third-authentication in order to construct the assessments system for better supervision of security outsourcing risk in accordance with the risk management policy in our country.

Key words: information security outsourcing; risk management; risk assessment

(上接第 59 页)

参考文献:

[1] 龙玉其. 中国收入分配制度的演变、收入差距与改革思考[J]. 东南学术, 2011(01): 103-114.

[2] 张清太. 居民收入差距扩大与分配制度缺陷分析[J]. 管理学刊, 2010(02): 22-26.

[3] 赵雪峰. 拉美国家缩小收入差距的社会政策及启示[J]. 中国经贸导刊, 2011(05): 45-47.

[4] 成学真, 李萍. 金融发展与城乡收入差距的实证研究[J]. 统计与决策, 2011(03): 134-136.

[5] 沈燕. 收入分配不平衡令相对贫困突现[EB/OL]. 路透中文网 http://cn.reuters.com/article/chinaNews/idCNCHINA-2644020100714.

[6] 作者不详. 农村经济绿皮书: 城乡居民收入差距仍在扩大[EB/OL]. 中国网. http://news.china.com.cn/txt/2011-04/19/content_22396404.htm.

Analysis of Imbalance of Income Distribution in China

LU Jian-hua

(Professional School of Transportation Technologies of Hebei Province, Shijiazhuang 052160, China)

Abstract: While China has kept a steady and fast economic development in recent years, the imbalance in income distribution among its citizens in different areas and different trades has become a serious social problem, arousing grave concerns from both the government and the society. In order to maintain the social stability, implement the concept of scientific development, realize a long-lasting economic development and construct a harmonious society, China must solve the problem of income imbalance. The problem of income distribution imbalance is explored in this paper from four respects including the imbalances between the citizen income and GDP increase, between rural and urban citizens, between different trades and different areas of the country, discussing the status quo and the causes of the problem and giving advice for mitigation of it.

Key words: income distribution; income gap; distribution system; reform