

影响网络信息安全的组织因素辨识

周荔,王樱^①,蒋娟^②

(南华大学 经济管理学院,湖南 衡阳 421001)

[摘要] 影响网络信息安全的组织因素主要有组织目标、组织结构、组织管理、安全文化和培训,运用问卷调查采集数据,使用探索性因子分析对影响网络信息安全的组织因素进行识别,并应用验证性因子分析方法予以验证。结果显示:安全文化与组织目标、组织管理、组织结构的相关性,组织管理与培训、组织结构之间的相关性均较强。这种相关性突出了安全文化和组织管理对网络信息安全的重要性。

[关键词] 网络信息安全; 组织因素; 结构方程

[中图分类号] TP393 **[文献标识码]** A **[文章编号]** 1673-0755(2012)06-0058-05

随着计算机网络技术的日益更新,社会信息化程度的不断提高,网络信息业已成为社会经济发展和人们日常生活中不可或缺的工具。网络信息系统在各类组织中得到了广泛的应用,使得许多组织对网络信息的依赖性不断增强。然而,网络信息安全问题也日益尖锐:网络黑客、木马、病毒、恶意代码、物理故障、人为破坏等均直接威胁到国家的安全、企业的秘密、个人的隐私等诸多方面。

面对日益尖锐的网络信息安全矛盾,人们在不断地探索和研究防范信息系统威胁的技术和方法。尽管网络信息安全技术从防病毒、防火墙技术到加密技术日趋完善,网络信息安全产品从杀毒软件到监听查杀木马软件日趋成熟,网络信息安全事故却依然频繁发生。

国内外大量文献研究发现,技术失误和人因失误不再是导致网络信息安全问题发生的最终答案。在典型的复杂人机系统——网络信息系统中,高集成化的设备,高密度的人员,整个系统已经成为一个开放复杂的宏观巨系统。根据事故致因理论,研究这样的巨系统的安全问题,可以发现导致系统不安全的因素(事故发生的因素)主要是人和设备(其它的因素都是由人和设备衍生出来的)^[1-4]。众所周知,设备是由人设计和使用的,所以保证系统安全的根本应该从人的角度入手。由于人具有不可能脱离

其生活的组织独立存在的社会性,所以预防与减少组织层面的失误已是确保网络信息系统安全运行亟需解决的重要问题。

一 影响网络信息安全的组织因素分类

(一) 组织因素分类基础

国内外各科研机构、学者一直致力于从不同视角对影响系统安全的组织因素分类分析,或从组织绩效角度,或从安全评价角度,或从人因可靠性和人误角度^[5-6]。

如 OECD/NEA 基于不同的理论与方法发展了评价组织安全绩效的重要组织因素分类,共分为 12 类:外部影响、目标和战略、管理功能与监督、资源分配、人力资源管理、培训、工作协作、组织知识、程序化、组织文化、组织学习、交流^[7]。张力和章逸民等在对核电厂进行安全评估时将核电厂人因及组织管理安全因素划分为安全目标与方针、人员配备与资格、组织机构与管理、配置控制、培训、职业健康、运行经验反馈、质量保证、人一机接口、遵章守法等 10 类 19 个要素^[8]。在对航空、石油工业、医疗等领域的事故调查后,Terry L、Scott A. Shappell 等用人的可靠性和人误分析方法,对影响人的活动的组织因素进行了分类^[9-10]。

组织因素的界定,基于不同的需求目标而存在差异;组织因素的分类,基于不同的角度而不同。

[收稿日期] 2012-06-16

[基金项目] 衡阳市社会科学基金项目“网络信息安全的组织因素研究——以衡阳市为例”资助(编号:2010D009);湖南省教育厅科研基金项目“基于任务上下文的信息检索多维匹配研究”资助(编号:11C1098)

[作者简介] 周荔(1980-),女,湖南郴州人,南华大学经济管理学院实验师。

①湖南信息职业技术学院讲师。②南华大学经济管理学院讲师。

(二)组织因素分类分析

本文界定的组织因素是指影响网络信息系统安全的、导致信息安全问题概率增加的、潜在于组织中偏离组织期望的组织过程缺陷或不良状态。网络信息系统是典型的复杂人机系统,根据国内外关于组织因素分类的文献研究成果,及 ISO27001:2005 中关于组织用于信息资产风险管理,确保组织信息安全应包括为制定实施、评审和维护信息安全策略所需的组织机构、目标、职责、程序、过程和资源的标准,结合网络信息安全的特征,对组织因素分类如下:

1、组织目标

组织围绕目标而建立,目标是开展各项组织活动的依据和动力。包含以下因素:(1)战略目标中的网络信息安全目标,组织的信息安全目标是实现组织追求高绩效目标的子目标之一,组织只有达到了信息安全的目标,才能真正实现组织的高绩效目标。(2)信息安全目标的优先次序,目标的优先次序即当存在诸多目标时,如何确定优势目标,使之形成优势动机。若不能形成优势目标,则会分散注意力,使组织无法集中能力去解决首要问题,将会影响组织目标的实现,甚至产生安全隐患。

2、组织结构

组织结构是组织中正式确定的使工作得以分解、组合和协调的框架体系,是组织内部分工与协调的基本形式。为实现组织目标,良好的组织结构是保证任务有效完成的最基本的前提条件。网络信息系统中的安全问题应当通过一定的组织功能去实现其既定的目标,合理的信息安全组织结构是保证组织网络信息安全管理的前提。

根据组织结构的定义,结合 IAEA 组织结构分类和网络环境下信息安全管理组织结构设计原则,本文将影响组织结构的因素分为信息安全工作组织、权力与责任、交流、资源。

3、组织管理

组织管理是一个组织为目标的实现而配置的组织、计划、指挥、监督、协调、控制的过程或活动。Gartner Group 曾经在一份安全报告中指出:“各类令企业损失惨重的安全违规事件归根到底都是人造成的,并且发展成为物理安全和人员的问题。IT 安全部门试图用技术方法来解决这些安全问题是行不通的。”究其原因在于信息安全是管理过程。

网络信息安全工作中的组织管理主要有:安全制度的建立、安全策略的制订、行为的规范、监督管理的执行等方面。

4、安全文化

安全文化是组织文化的一个子集,通常被定义为安全价值观与安全行为的总和^[11]。有着良好安全文化的地方总伴随着较低的事故率,因此,是否形成了良好的安全文化氛围会影响网络信息安全事故的发生率。具体体现在网络安全文化、领导层的意识和态度、员工个人的意识和态度及员工间的和谐度等方面。

5、培训

培训指使员工具有一定技能和知识的过程,即通过识别任务的特性和功能、识别安全地 and 有效地完成任务所需的知识、能力和才干,以教育和练习等方式提高人员的知识、能力和经验等各方面素质的过程,只有具有一定技能和知识的员工才能保证安全有效地完成工作。包括培训的内容和培训队伍的素质。

二 组织因素的辨识

为辨识影响网络信息安全的组织因素,笔者设计问卷、收集数据,并对收集到的数据进行探索性因子和验证性因子分析。

(一)探索性因子分析

为避免出现遗漏和个人理解偏差,较为全面地识别影响网络信息安全的组织因素,在研究的前期,对教育、通信、商业、医院等行业中从事网络信息工作的专业人士进行咨询,征求他们对影响网络信息安全的组织因素分类及其测量指标的意见和建议。根据组织因素分类相关理论基础及对专业人士的咨询结果,设计预试调查问卷,分别发给各行业中从事网络信息工作的人士进行调查补充、修订组织因素分类及其观测变量。预试阶段获得问卷 36 份,应用 SPSS17.0 软件对回收的有效预试调查问卷进行探索性因子分析,依据柳恒超关于模型选择原理与方法的研究^[12],删除分析结果中载荷因子小于 0.5 的观测变量,得到正式调查问卷中的组织因素分类框架,如图 1 所示。

(二)验证性因子分析

正式调查中,问卷以电子问卷方式发放,调查对象是各行业从事网络、信息管理的相关人员,共发放 200 份问卷,回收 127 份有效问卷。采用结构方程软件 AMOS17.0 对影响网络信息安全的组织因素进行验证性分析。

1、建立验证性因子模型

在探索性因子分析基础上对识别的影响网络信息安全的组织因素分类建立模型,并假设各个因子之间都存在相关性,如图 2。

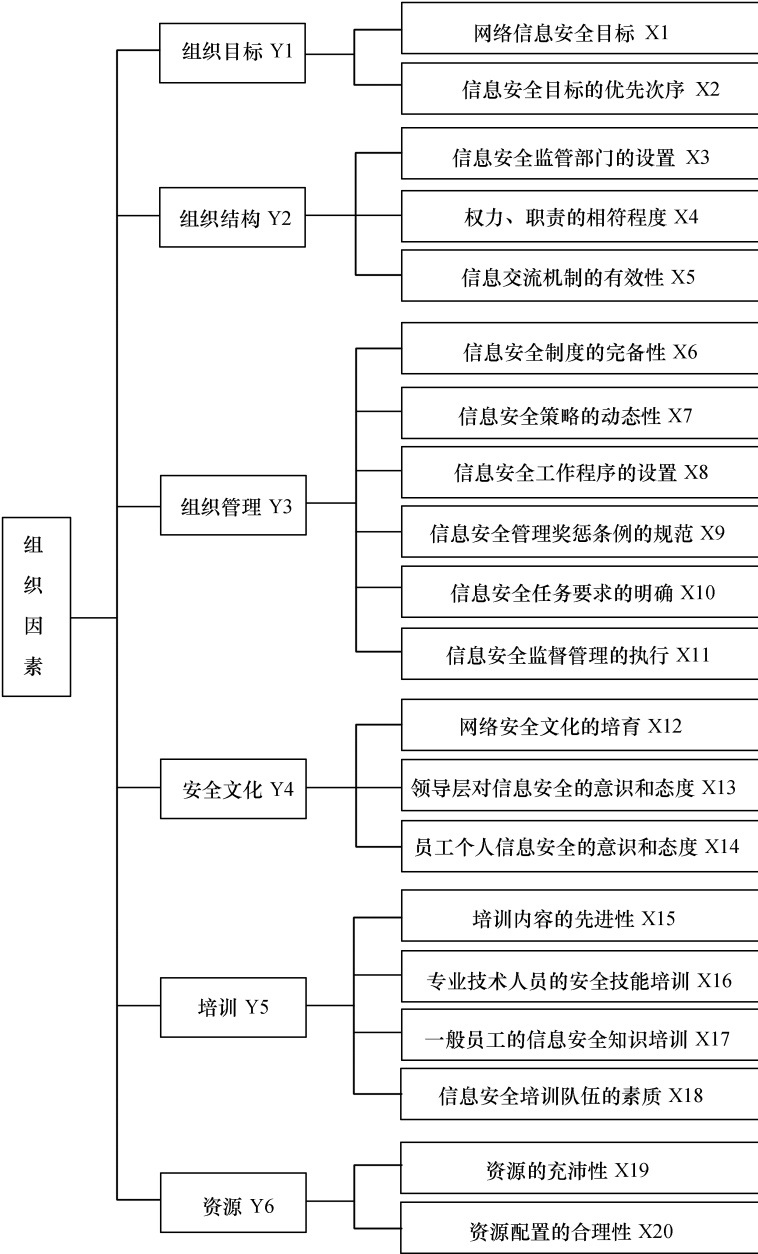
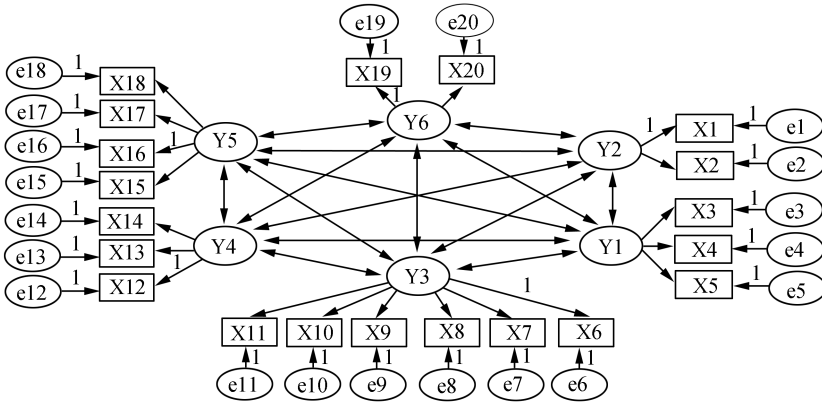


图 1 影响网络信息安全的组织因素分类框架



注：X 为观测变量或因子指标；y 为潜在变量或因子

图 2 验证性因子模型

2、模型的拟合

型的拟合程度,如表 1。

本研究从下表中八个常用的拟合指数来反映模

表 1 拟合指数评价标准及模型拟合指数计算结果(P=0.00)

指数类别	拟合指数	评价标准	计算结果	解释
绝对拟合指数	X ²	越小越好	X ² /Df =2.075	大于 2 但小于 3,说明模型拟合得不好,但可以接受
	GFI	介于 0-1 之间,越接近 1 越好,一般大于 0.9	0.781	模型有很大的修改空间
	RMR	越小越好,一般小于 0.05	0.175	模型有不足之处
	RMSEA	越小越好,一般小于 0.08	0.093	模型拟合效果不好
省俭拟合指数	PGFI	介于 0-1 之间,越接近 1 越好,一般大于 0.5	0.576	大于 0.5,符合标准
增值拟合指数	CFI	介于 0-1 之间,越接近 1 越好,一般大于 0.9	0.743	模型有很大的修改空间
	NFI	介于 0-1 之间,越接近 1 越好,一般大于 0.9	0.616	模型有很大的修改空间
	TLI	介于 0-1 之间,越接近 1 越好,一般大于 0.9	0.685	模型有很大的修改空间

注:X²(卡方)受样本量影响较大,样本量越大 X² 越大,好的模型应有较小的 X²。由于 X² 值受自由度 Df 的影响比较大,人们常把 Df 作为评价模型拟合度的指标,一般认为当 X²/Df<2 时说明模型与数据拟合得好。美国社会统计学家卡米尼斯和马克依维尔认为,卡方值与自由度之比在 2:1 到 3:1 之间是可以接受的。

综合以上拟合指数,说明模型与数据之间的拟合效度很差,需要修正模型以获得较好的拟合。

3、模型的修正

从 AMOS 提供的修正指数表及相关性矩阵中数据的分析结果显示 X8 和 X9、X9 和 X10、X8 和 X10、X16 和 X17 四对指标之间的相关性很强。因为 X8 信息安全工作程序的设置、X9 信息安全管理奖惩条例的规范、X10 信息安全任务要求的明确同属于规程、X16 专业人员的信息安全技能培训、X17 一般员工的信息安全基础知识培训同属于培训内容的全面性,说明将它们分开设置题目或不分开并没有显著的差别。因此,考虑将 X8、X9、X10 合并为“有关信息安全管理规范的完备性”,将 X16 和 X17 合并为“培训内容的全面性”。处理后从拟合指数修正结果发现,各拟合指数都得到了一定的改善,但是部分指数仍未达到要求。由于本研究的模型是基于对专业人士关于影响网络信息安全的组织因素的分析进行探索性因子分析之上建立的,不切实际的修改模型,虽能得到好的拟合指数,但会得出没有理论意义的模型,故不再修正模型。本研究中虽有一些指数没有达到要求的拟合度标准,而一些指数已经达到,未达到要求的指数大都接近标准,所以整个模型还是具备一定参考价值。

经验证性因子分析后,影响网络信息安全的组

织因素分类体系如表 2:

表 2 影响网络信息安全的组织因素指标体系

影响因素	子因素
组织目标因素	网络信息安全目标
	信息安全目标的优先次序
组织结构因素	信息安全监管部门的设置
	权力、职责的相符程度
	信息交流机制的有效性
组织管理因素	信息安全制度的完备性
	信息安全策略的动态性
	信息安全管理规范的完备性
	信息安全监督管理的执行
安全文化因素	网络安全文化的培育
	领导层对信息安全的意识和态度
	员工个人对信息安全的意识和态度
培训因素	培训内容的先进性
	培训内容的全面性
	信息安全培训队伍的素质
资源因素	资源的充沛性
	资源配置的合理性

三 结论

从模型拟合的情况以及显著性 P 值来看,模型基本上与数据相拟合,其结果显示:安全文化与组织目标、组织管理、组织结构的相关性,组织管理与培

训、组织结构之间的相关性均比较大。这种相关性突出了安全文化和组织管理的重要地位,说明安全文化作为组织中的一种向心力和精神支柱,组织管理作为员工在组织中行事的依据对网络信息系统安全运行的重要性。

[参考文献]

- [1] Dr Eugene Schultz. The human factor in security[J]. Computers&Security, 2005(24): 425-426.
- [2] Charles Cresson Wood, William W, Banks Jr. Human error: an overlooked but significant information security problem[J]. Computers&Security, 1993(12): 51-60.
- [3] Martin Bean. Human error at the center of IT Security Breaches[EB/OL]. [2009-08-10]. <http://www.newhorizons.com/elevate/Network%20Defense%20Contributed%20Article.pdf>.
- [4] 刘绘珍. 影响复杂人机系统安全的组织因素分析[D]. 衡阳: 南华大学硕士学位论文, 2007.
- [5] 李鹏程, 肖东生, 陈国华, 等. 高风险系统组织因素分类与绩效评价[J]. 中国安全科学学报, 2009, 19(2): 144-151.
- [6] 刘绘珍, 张力, 张玉玲, 等. 影响系统安全的组织因素分类分析[J]. 核动力工程, 2009, 30(4): 59-63.
- [7] ETF/PWG No. 1. Organizational factors-identification and assessment (NEA/CSNI/R(98)17)[Z]. Issy-les-Moulineaux: OECD/NEA, 1998.
- [8] 张力, 章逸民, 吴当时, 等. 核电厂人因及组织行政管理安全审查体系[J]. 中国安全科学学报, 2003, 13(6): 4-7.
- [9] Terry L. von Thaden, Douglas A. Wiegmann, Scott A. Shappell. Measuring Organizational Factors in Airline Safety[R]. AHFD-03-11/FAA-03-3, University of Illinois at Urbana-Champaign 1 Airport Road Savoy, Illinois 61874, 2004.
- [10] Chang Y H J, Mosleh. A Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. Part 4: IDAC causal model of operator problem-solving response[J]. Reliability Engineering and System Safety, 2007, 92(8): 1061-1075.
- [11] 唐枫. 倡导安全文化提高安全管理[J]. 工业安全与防尘, 2001, 27(1): 38-40.
- [12] 柳恒超. 结构方程模型应用中模型选择的原理和方法[J]. 心理学探新, 2007(1): 75-78.

Discrimination of Organization Factors Influencing Network Information Security

ZHOU Li, WANG Ying, JIANG Juan

(University of South China, Hengyang 421001, China)

Abstract: The research discusses organizational factors which possibly trigger the problem of network information security. By collecting data from questionnaire survey, adopting exploratory factor analysis to discriminate the organizational factor, and using structural equation modeling to confirm these factors, it is concluded that safety culture is closely connected with organization goal, organization management and organization structure. Also, the results show organization management has a strong connection with orientation and organization structure. The dependency underlines the importance of safety culture and organization management.

Key words: network information security; organizational factor; structural equation