国民信息安全素养评价指标体系构建研究

罗 力
(上海社会科学院 信息研究所,上海 200235)

摘要:信息安全已成为信息时代国家总体安全的基石,是当下中国必须认真严肃面对的一个重大问题。要想实现"以人为本"的信息安全管理,第一步就要重视国民信息安全素养。文章对信息安全和信息安全素养的内涵进行剖析,对国内外信息安全素养研究和推广项目进行回顾,指出信息安全素养应该包括信息安全意识、信息安全知识、信息安全能力、信息伦理道德等内容,信息安全素养应在信息素养的概念体系中占据重要位置。最后根据信息安全素养内涵,运用过程—目标结构法构建了国民信息安全素养评价指标体系。

关键词:信息安全;信息安全素养;信息安全保障;评价指标体系
中图分类号:C32 **文献标志码**:A **文章编号**:1008-5831(2012)03-0081-06

一、引言

目前,随着中国社会信息化程度的全面提升,网络与信息系统已经成为国家的关键基础设施,其基础性、全局性作用进一步增强,信息资源在国民经济发展中的作用与日俱增,谁能够及时掌握丰富的信息资源,谁就能在政治、经济、军事和文化等方面占据优势地位。但与此同时,信息安全问题日益多样化、复杂化。针对网络和信息系统的攻击活动以及网络与信息系统自身的安全问题,严重影响着金融、电力、交通等关键基础设施的正常运转,病毒传播、网络攻击、网络泄密等案件逐年上升。信息安全问题已经不仅仅是一个技术问题,也不仅仅是一个社会问题,而是涉及到政治、经济、社会、文化、军事等方方面面,进而上升成为国家全局性战略问题。中共十六届四中全会已将信息安全列入国家安全的四大重要组成部分之一,另外三大部分为政治安全、经济安全和文化安全。据北京谷安天下科技有限公司发布的《2010 企业员工信息安全意识调查报告》显示,42.8% 的受访者认为个人信息安全意识不足是最大的信息安全隐患,然后依次是缺少安全制度或现有制度未落实、投入或人员不足或缺乏信息安全培训、安全产品功能不足和其他。而对于目前有效保护信息安全面临的最大障碍是普遍缺乏信息安全意识,其他依次是管理水平落后、技术不过关、法律不健全、信息安全人才不够和其他障碍。报告进一步显示,中国企业员工普遍缺乏信息安全意识[1]。另外在 RSA2011 信息安全大会上,不少信息安全专家不约而同地提出了一个引人关注的问题,即众多缺乏安全意识的员工,正在成为黑客突破企业安全防护时,最大也最难修补的漏洞[2]。2012年初CSDN和天涯等众多网站用户数据

收稿日期:2012 - 01 - 09
作者简介:罗力(1982 -),男,浙江台州人,上海社会科学院信息研究所助理研究员,博士,主要从事信息计量与信息安全研究。

大规模泄露事件的主要原因是用户习惯使用一号多用的账户和密码,当个别网站个人资料泄露后,直接导致了多个网站的账户同时被曝光[3]。因此,加强对国民信息安全素养进行评价,让广大国民认识到自身信息安全素养的现状,并有效提升其信息安全素养是亟待解决的重要问题。

二、信息安全与国民信息安全素养的内涵

信息安全是一个既古老又年轻的话题,包含的范围很大,大到国家政治军事科技等机密安全,小到防范企业商业机密被窃取、个人信息泄露等。信息时代的到来更加凸显了信息安全的重要性和紧迫性。目前一般从狭义和广义两个方面理解信息安全。狭义的信息安全是指信息本身的安全问题,基本包括信息的保密性、完整性、可用性、可控性及可靠性五个方面。保密性是指确保信息仅为那些被授权者获取使用;完整性是指保护信息不被删除、修改、伪造、乱序等以确保其完整准确;可用性是指保证被授权者可以按需获取使用信息;可控性是指信息和信息系统处于安全监控管理状态;可靠性是指信息系统在规定条件下完成特定功能的概率。广义的信息安全是指社会信息化状态和信息技术体系不受外来威胁和侵害,以此维持国家政治、军事、经济、科技、文化、社会生活等系统正常运行的状态。广义的信息安全包括政治信息安全、经济信息安全、科技信息安全、军事信息安全、文化信息安全、生态信息安全、公共信息安全等内容[4]。

国民信息安全素养是指在信息化、网络化环境下,国民对信息安全的认识,以及对信息安全所表现出的各种综合能力,包括信息安全意识、信息安全知识、信息伦理道德和信息安全能力等具体内容[5]。它是信息社会中信息素养的重要组成部分,已成为信息社会人类生存立足的重要条件。信息安全意识是指人们能够认识到信息安全在工作、学习和生活中的重要性,对信息安全有一定的敏感性和洞察力,熟悉常见安全威胁的识别方法以及有效的安全保护措施。信息安全知识是指人们熟悉信息安全的基本概念和基本理论框架,了解计算机安全和网络安全的最新技术。信息伦理道德是指人们在获取、利用、加工和传播信息的过程中必须遵守一定的网络信息伦理道德规范,自觉抵制网络盗版、计算机病毒、电脑黑客等行为。笔者所讨论的信息安全素养的内涵比信息安全意识更加丰富,不仅包含关心和维护信息安全的意识取向,更包含后续各种防护能力、信息安全伦理道德等内容。信息安全素养与计算机素养有所不同,后者主要指个人使用计算机所需要的各种基础知识。另外信息安全素养的养成是长期"修习"的结果,并非天生就有,也不能一朝一夕就形成。信息安全素养的形成有一个程度变化的过程,即从低到高逐步发展的过程。

三、国内外信息安全素养研究与推广进展分析

国内外文献调研表明,欧美等西方国家在信息安全素养研究与培养方面走在了前面。NIST(National Institute of Standard and Technology,美国国家标准技术学会)推出的 Special Publication(SP)800 – 50[6]标准提到,信息安全的关键因素是人而并非科技。信息安全素养课程体系采用信息安全基础(ABC's of Information Technology Security)中的相关知识,具体并详细说明信息安全的基本概念,提供给人们学习并能遵守的信息安全的一般性主题和概念,分别是法律和规范、组织与信息技术安全、系统互联和信息共享、敏感性、风险管理、管理控制、获取/开发/安装/执行控制、运行控制和技术控制等九大类。在 SP500 – 172 中提出,各组织机构应对所有管理、使用计算机系统的作业人员,实施强制且定期的计算机安全认知的训练[7]。Whitman and Mattord 指出,员工位列公司信息资产安全的首要威胁因素,信息安全意识教育和培训是公司安全教育的环节之一。Czernowalow 认为,员工的安全培训成本远小于潜在损失。信息安全控制只有在员工意识到安全的重要性时才能发挥作用。Drevin、Kruger 和 Steyn 根据信息安全的定义认为信息安全意识评价指标体系应该包含六个方面,这应作为制定信息安全意识培训项目计划的依据,并最终影响组织建立信息安全文化[8]。Aggeliki Tsohou、Maria Karyda 等人针对目前信息安全意识培训与信息安全管理相脱节的情况,认为这两个过程应该放在一起讨论,信息安全意识培训在信息安全管理中要占据重要位置[9]。截止 2011 年 12 月,笔者对中国知网、万方数据库和百度等搜索引擎检索"信息安全素养"的论文,发现题名包含"信息安全素养"的只有三篇。而检索"信息安全意识"的结果稍多,但理论研究成果更少。刘枫认为,信息安全素养是在信息化条件下,人们对信息安全的认识,以及对信息安全所表现出的各种综合能力。吴倩萍对政府机关各层级人员的信息安全意识和其行为的关系进行了研究[10]。虽然其他"信息安全"研究的有关成果中有涉及如何改善信息安全意识问题,但研究大多以定性描述为主,研究深度亟待拓展,所提出的对策操作性有待强化。

美国国防部制订并实施了对军人、文职及合同制信息人员的全方位教育、培训计划。对信息系统

的使用者规定了必须掌握的最低限度的信息安全领域的基本知识,没有这些必备的基础知识,工作人员不能上岗工作,全体人员每年进行一次再培训。除此以外,秘密及非秘密系统的数据库管理员需要考取上岗合格证。为了完善培训方法,成立了"信息安全计划办公室"。国防部信息系统局制作与下发了许多含有教育课程资料的光盘及电影。为了提高高等院校在信息安全领域的教学质量,国家安全局成立了高校毕业生信息安全再教育中心。美国还设立了"国家网络安全意识月",即每年 10 月 1 日开始,举办一连串的网络安全意识的推广活动,教育美国民众、企业、学校与政府机构,保护他们的网络环境、计算机以及国家的关键基础建设,透过一些简单而更有效的步骤教育使用者远离最新的威胁,以及遇到可能的网络攻击事件时如何响应[11]。欧洲网络与信息安全局在《信息安全意识创新:目前实践和成果》调查报告中分析了欧盟中的组织和政府是如何看待信息安全意识和评价其影响的。该机构在另一份题为《提高信息安全意识》的文件中指出:"在所有的信息安全系统框架中,人这个要素往往是其最薄弱的环节。只有革新人们陈旧的安全观念和认知文化,才能真正减少信息安全可能存在的隐患。具备高度信息安全意识的个人和有效的安全措施,被视作信息系统和网络安全的第一道防线。"[12]英国政府内政部及国家高科技犯罪小组开展了提升广大青少年、家长及单位网络用户的安全意识活动,并联合了微软、赛门铁克等商业组织建立了活动网站。荷兰经济事务部为 6 – 18 岁的学生群体制定了一系列的网络安全意识提升计划。丹麦开展了旨在提升包括学生、家庭以及企业广大网络用户安全意识的 Net—Safe Now 活动[13]。澳大利亚联邦政府自 2001 年 9 月开始已制定增强全民信息安全素养的计划,这个计划覆盖各类组织以及各个知识层次的国民。中国至今尚无承担相应推广工作的机构,亦无全民信息安全素养提升计划的出台,只有部分地区和组织开展类似活动[14]。中国台湾从 2008 年开始于每年 12 月初举办为期一周的"全民安全周"推广活动,倡导对象由政府人员普及至学校、企业及民众,共同推动全民信息安全意识[15]。上海在 2011 年 10 月 13 日至 19 日举办了首届"信息安全活动周",加强全民信息安全防范意识,保障和促进上海智慧城市建设[16]。中山大学的信息与网络中心每个月都会举行信息安全意识的主题教育活动。上海交通大学网络信息中心也于 2008 年 11 月编写了《网络安全常见问题》宣传单在校园内发放。武汉大学已从 2005 年开始在全校陆续开设了 4 门通识选修课用于培养大学生的信息安全意识和提高他们基本的信息安全防护能力[17]。总体来说,目前国内研究大多以定性描述为主,研究方法有待改进,研究深度亟待拓展,所提出的对策操作性有待强化,更没有从评价指标体系和影响因素角度研究信息安全素养的内涵和培养工作,这对于信息安全管理研究和实践是一个非常大的缺陷,也和国内外信息安全研究逐渐重视管理视角和用户的现状不相符合。国内外信息素养的研究主要侧重于如何获取和利用信息解决问题,忽视了当前信息安全形势严峻背景下如何有效防护各种信息安全威胁的讨论。信息安全素养理应在信息素养的概念体系中占据重要位置。另外国内的信息安全素养推广和培训活动的范围与形式还有待加强。从理论和实践两个层面的国内外对比可以看出,中国必须真正重视信息安全素养的研究和培养工作。因此根据信息安全素养的自身特征和规律,确定一个科学合理且具有可操作性的评价指标体系,并以此为基础展开研究是当务之急和重要突破点。目前还没有从情报学角度对国民信息安全素养直接进行评价研究,国家社科基金也没有资助过这方面的研究项目。

四、国民信息安全素养评价的必要性

没有科学的评价,就没有科学的管理。国民信息安全素养的评价是对信息安全素养教育或培养过程中的自觉性反映,是国家信息安全保障体系建设中亟待解决的问题,具备一定的理论价值和现实意义。

第一,国民信息安全素养评价指标体系的建立具有理论价值和科学意义。虽然各学科领域都从不同角度出发直接或间接地对信息安全进行了研究,取得了一定的成果,但非常缺乏信息安全素养方面的研究。而在信息安全风险评估与管理领域,人员风险控制是重要组成部分。创建国民信息安全素养评价这一相对独立的交叉研究领域,可以集中各门学科的优秀研究成果,完善信息安全研究理论体系。

第二,国民信息安全素养评价指标体系的建立具有实践意义和现实作用。信息安全素养评价对于推动网络环境下的国民信息安全素养教育和培养工作具有指导意义。只有进行信息安全素养评价标准研究,构建一套科学合理的信息安全素养评价指标体系,相关部门和机构才能更准确、真实地了解当前国民的信息安全素养水平,发现其薄弱环节,才能洞悉目前信息安全素养教育的不足,有针对性地制定课程计划和培养方案,改进信息安全素养教育,从而

更好地指导中国开展普及化的信息安全素养教育和培训项目,满足广大国民自身的需求,进一步从人员上落实国家信息安全保障体系建设工作,提升国家信息安全保障体系的总体水平,有效回应 2003 年中办 27 号文关于明确加强信息安全保障工作的总体要求和全面工作部署精神。

五、国民信息安全素养评价的原则

"评价"是评定价值的简称。从本质上说,评价是一种价值判断活动,是用一种能够获得公众认可的价值标准衡量和判断事物的价值与优点,是对客体满足主体需要程度的判断。指标就是将抽象的、难以测量的社会概念翻译成可以考察、分析的操作性术语。对国民信息安全素养的评价是对国民在面临信息安全问题时的应用能力的价值判断,相应的指标体系就是要将评价目标中定性的难以测量的部分进行量化、细化,把抽象的、原则性的目标具体化、可操作化,使评价能够更加准确更加容易的进行。因此,需要按照下列原则选择和组织[18]。

(一)科学性原则

任何评价体系都应该建立在一定的理论基础之上,科学性是构建评价体系最基本的原则。国民信息安全素养评价指标体系框架及各级指标的确定应该由强有力的信息安全理论以及学科教育标准作为支撑,应严格从信息安全素养的概念内涵出发,客观揭示影响国民信息安全素养的各个要素。各级指标相互照应又彼此独立,指标间具有清晰的逻辑层次关系,层层递进,环环相扣。上下级指标具有一致性,同一层次的指标不雷同,外延不交叉,确保整个评价指标体系构成一个科学完整的逻辑系统。

(二)可操作性原则

评价指标体系应能直接测量,简便易行,具有良好的可操作性。在指标描述时应从非信息安全专业人士的视角展开,尽量避免空而全的指标,尽可能多地通过实例或注释的形式将指标说明清楚。

(三)导向性原则

国民信息安全素养评价指标体系不仅应反映信息安全领域最新进展,同时,还应该对国民信息安全素养的自主学习与培养有明确的导引和参考作用。

(四)动态性原则

由于信息安全素养是一个动态发展的概念,不同的时期其内涵和外延也不同,因此所构建的指标体系应具有一定的前瞻性,不仅适用于现阶段,还能在时间上延续,在内容上拓展。

六、国民信息安全素养评价指标体系的构建

在明确信息安全素养内涵的基础上,信息安全素养评价体系的构建应结合信息安全素养标准,按照系统工程的思想,将总体目标层层分解。国内外处理类似问题主要有三种方法:列举描述法、过程结构法和目标描述法。以信息安全素养为例,列举描述法是根据个人或组织的理解,以一种平铺直叙的方式描述信息安全素养的内涵,其弊端之一就是对信息安全素养的不同理解会导致信息安全素养内涵的随意收缩和扩张,弊端之二是缺乏对各个组成要素之间逻辑关系的描述。过程结构法是在详细了解信息安全素养的概念基础上,按照信息安全需求、信息安全知识储备、应对处理等一个完整的信息安全行为过程而展开。信息安全行为过程由很多个环节构成,这些环节紧密相连环环相扣。信息安全素养的完整内涵由这些环节对信息主体在知识、能力、技能等方面要求构成。由于信息主体的信息安全行为在内容和秩序上都保持较高的稳定性,具有稳定的内容结构和秩序结构,因此使用这种方法推导的信息素养内涵相对全面和稳定。但在信息安全行为过程中起到引导作用的情感态度与价值观因素(信息安全意识和信息伦理道德等),贯穿于整个信息安全行为过程当中,而过程结构法不能将其融入某一个具体的过程,只能将其一一列出。目标描述法是在充分理解信息安全素养概念内涵和外延的基础上,对国民信息安全素养教育目标的明确概述。目标描述法对信息安全素养的高度抽象和概括是信息时代社会对人们的信息安全素养的要求,即达到信息安全意识、信息安全知识、信息安全能力、信息伦理道德四个方面的要求,就可被认为具备较高的信息安全素养。目标描述法的优点是符合中国人高度概括的思维习惯。但该方法也有其缺点,一是这种描述方法缺乏可操作性,二是在每一层次中所包含的具体内容不够清晰[18]。

过程结构法是国外处理类似问题的思考方式,目标描述法则是国内应用的主要方式。尽管这两种方式的思路不同,但有着相同的认识对象,因此在本质上能够将他们统一。比如过程结构理论中明确信息安全需求与目标结构理论中的信息安全意识可以视为同一方面的内容;而目标结构理论中的信息安全能力与过程结构论中的信息安全应对处理等能力相对应。将上述两种结构结合便构成了信息安全素养的过程——目标结构体系。在过程—目标结构体系中,以信息安全素养的目标为核心,在信息安全行为的整个过程中都体现着信息安全素养的目标,更好地展现了信息安全素养的内涵。由于国内还没有具有权威性的信息安全素养标准,因此,笔者在借鉴

美国 NIST SP800－16 信息安全 ABC(ABC's of Information Technology Security)的基础上,结合过程—目标结构法和层次分析法构建国民信息安全素养评价指标,力求每项指标反映信息安全素养的内涵,既不重复又互相补充,从而构建信息安全素养评价指标体系。为了简化分析过程,本文只构建二级指标体系,暂时不确定权重,具体如表 1 所示。信息安全素养是一个能力集群,它由各种各样的能力构成,其中包含广大国民必须掌握的核心能力,而每项能力又可细分为若干子能力。笔者将信息安全素养分为三层:目标层、准则层和指标层,其中 L1、L2、L3、L4 层构成了上述核心能力。该体系能够较为全面地反映国民信息安全素养应该包含的各项能力,同时符合中国民众所处的网络化大环境。

表 1　国民信息安全素养评价指标体系

目标层	准则层	指标层
国民信息安全素养评价标准 L	信息安全意识 L1	了解信息安全在信息社会的重大作用 L11
		了解信息安全面临的严峻形式与挑战 L12
		了解人为原因是造成信息安全的重要因素 L13
	信息安全知识 L2	了解各种病毒、木马危害及最新信息安全威胁 L21
		了解信息保护技术基础知识及相关概念 L22
		了解移动介质(优盘、移动硬盘等)使用不当会泄密 L23
		了解信息存储和获取的各种规定 L24
		了解删除信息需遵守特定规定 L25
	信息法律伦理 L3	了解信息安全相关的法律法规和政策 L31
		了解信息安全保护的职责与义务 L32
		能尊重知识产权(如抵制盗版)、抵制不良信息、软件等 L33
	信息安全能力 L4	能保护物理设施的安全性 L41
		能正确设置密码确保信息私密性 L42
		能防范计算机网络犯罪和计算机病毒等恶意攻击 L43
		能防范垃圾信息的入侵(如垃圾短信、邮件等)L44
		能定时备份重要资料 L45
		能从多渠道获取解决信息安全问题的手段 L46

七、结语

信息安全是当下中国必须认真面对的一个重大问题,如果处理不慎,将严重影响中国信息化健康发展,甚至可能严重威胁中国经济安全乃至国家安全。当前那些由最先进的信息安全设备组成的铜墙铁壁由于"人"的缺位很可能不堪一击。因此,要实现"以人为本"的信息安全管理,第一步就要加强国民信息安全素养的教育和培养。笔者运用过程—目标结构法构建了国民信息安全素养评价指标体系,可以在一定程度上帮助建立信息安全素养教育的内容和目标,但因时间有限,尚未运用层次分析法和模糊综合评判法确定指标权重,应用于评价实践中,这是下一步将要努力研究的内容。

参考文献:

[1]国内首份员工信息安全意识调查报告问世[EB/OL]. [2011－10－23]. http://www.enet.com.cn/article/2010/0915/A20100915729062.shtml.

[2]从索尼数据泄漏事件看网络安全的"人祸"[EB/OL]. [2011－10－23]. http://article.pchome.net/content－1331343.html.

[3]密码泄露事件暴露网络信息安全弊端[EB/OL]. [2012－01－01]. http://finance.jrj.com.cn/tech/2011/12/28213811933543.shtml.

[4]张静. 国家安全中的信息安全研究[D]. 成都:电子科技大学硕士学位论文,2005:3－4.

[5]刘枫. 大学生信息安全素养分析与形成[J]. 计算机教育,2010(21):77－80.

[6]NIST. Building an information technology security awareness and training program, NIST special publication 800－50 [EB/OL]. [2012－01－01]. http://csrc.nist.gov/publications/nistpubs/800－50/NIST－SP800－50.pdf.

[7] NIST. Computer security training guidelines, NIST special publication 500 - 172. U. S. Government Printing Office [M]. Washington, November ,1989.

[8] DREVIN, KRUGER, STEYN. Value-focused assessment of ICT security awareness in an academic environment [J]. Computers & Security,2007(26):36 - 44.

[9] AGGELIKI T, MARIA K, SPYROS K, et al. Aligning Security Awareness With Information Systems Security Management[M]. MCIS Proceedings,2009:865 - 876.

[10] 吴倩萍. 政府机关个人信息安全认知与行为之探讨[D]. 国立台北大学公共行政暨政策学系硕士在职专班硕士论文, 2006.

[11] 奥巴马宣布 10 月为美国国家网络安全意识月[EB/OL]. [2011 - 12 - 20]. http://www. hackbase. com/news/2009 - 10 - 12/30075.

[12] 蒋莉,杨培静. 欧美国家如何培养网络安全意识[J]. 中国教育网络,2008(7):48 - 49.

[13] 杨培静. 欧洲国家安全意识提升计划[J]. 中国教育网络,2008(11):41 - 44.

[14] 熊四皓. 澳大利亚联邦政府信息安全管理体制[J]. 网络安全技术与应用,2004(3).

[15] 全民资安推广网[EB/OL]. [2011 - 12 - 30]. http://www. cybersecurity. tw/.

[16] 徐瑞哲. 全国首个信息安全活动周启动[EB/OL]. [2012 - 01 - 01]. http://www. people. com. cn/h/2011/1014/c25408 - 3797252916. html.

[17] 彭国军,黎晓方,张焕国. 信息安全意识培养应纳入大学生素质教育培养体系[J]. 计算机教育,2008(31):44 - 45,31.

[18] 曹秋花. 师范院校本科生信息素养评价指标体系研究[D]. 山东:曲阜师范大学硕士学位论文,2010:15 - 20.

Exploreration of the Evaluation Indicator System of National Information Security Literacy

LUO Li

(*Institute of Information, Shanghai Academy of Social Sciences, Shanghai 200235, P. R. China*)

Abstract: Information security has become the cornerstone of the overall national security in the information age and it is a serious problem China must cope with. In order to realize People-oriented information security management, the first step is to pay attention to the national information security literacy. The article analyzes information security, information security awareness and information security literacy, gives a review of the existing research findings and propaganda programs at home and abroad. Information security literacy should include information security awareness, information security knowledge, information security ability, information ethics, and information security literacy should play a key role in the system of information literacy. In the end, the article builds the evaluation indicator system of national information security literacy according to the concept of information security literacy.

Key words: information security; information security literacy; information security assurance; evaluation indicator system;

(责任编辑 彭建国)