doi:10.3969/j.issn.1671-5152.2014.08.001

燃气行业信息安全体系建设方法及在北京燃气的实践

□ 北京市燃气集团有限责任公司（100035）王广清

摘　　要： 本文首先介绍了燃气行业信息化现状、分析了燃气行业信息安全存在的问题，然后介绍了企业建立信息安全体系的思路和方法，并结合此理论在国内首次提出了燃气行业信息安全体系的构建方法；最后以北京燃气为例，对燃气行业信息安全体系建设方法进行了实践和应用，分析并总结了燃气行业信息安全体系建设成功的关键因素。

关 键 词： 燃气行业　燃气信息化　燃气信息安全　信息安全规划　燃气信息安全体系　工控安全

1　概述

近年来，燃气企业不断提高其信息化水平以支撑业务的高速发展，提升企业工作效率并优化业务运作模式，向公众提供高质量的服务。但是，作为传统能源行业，燃气企业在利用信息技术带来的优势时也必然需要承受先进技术带来的风险——信息安全问题。

2010年6月，“震网”病毒悄然袭击伊朗核设施的工业系统，“震网”是第一个被发现用于针对于政府的网络战争武器。2012年，美国国土安全部应急响应小组报告了198起针对重要基础设施的攻击，而2011年的攻击数量为130起（上升了52%）。据欧洲网络与信息安全局统计的数据，在2012年遭受攻击最多的行业为能源行业，占41%，其次为供水，占15%[2]。

燃气企业本身存在的信息安全问题、外部严峻的安全形势以及各种监管的压力都要求燃气企业尽快建设信息安全体系。本文将对北京燃气信息安全体系建设过程中的经验、方法进行整理，供燃气行业其他企业构建信息安全体系参考。

下文的“燃气企业”泛指国内绝大部分燃气企业，代表着国内燃气行业的主要情况。

2　燃气行业信息化现状及信息安全问题

2.1　燃气行业信息化现状

国内燃气企业的生产运营信息化建设开始于1996年左右，目前北京、上海、长春等多个大城市的管道燃气企业均成功完成生产运营信息化项目的建设，使企业运营过程控制程序化、模型化、智能化、集成化、网络化，监测、控制过程实现可视化和远程化，以期达到进一步理顺管理流程、提升管理水平和提高工作效率的目标。国内燃气行业信息化具有以下特点：

（1）企业的信息化建设已覆盖主要业务，但信息化缺乏有效整合，信息化的“孤岛效应”明显，企业信息资源没有得到有效利用。

（2）信息化管控能力薄弱，企业缺乏有效IT治理机制和行业的信息化标准规范指导，信息化在企业管理应用有待提高。

（3）信息化技术力量薄弱，企业的信息化建设

严重依赖于第三方服务。

（4）工业体系安全核心正在转变，由传统的物理安全正在向信息安全转移。

国内燃气企业已经基本完成了信息化“建设”的初期任务，已经建成了涵盖SCADA、GIS、OA、ERP、EAM以及用户管理系统等信息系统，而为了支撑燃气业务的高速发展，更有效的、安全的利用信息化体系，实现信息化的整合和管控必然成为企业未来信息化发展的主题，企业信息化发展路线也逐步由偏重建设转向偏重管控。信息安全作为信息化管控的主要组成部分，已成为企业必须面对的现实问题。

2.2 燃气行业信息安全问题

作为传统的能源行业，大部分燃气企业对信息安全比较陌生，缺乏主动有效的信息安全保障机制。下面从组织、策略和技术3个层面分析燃气行业信息安全存在的问题。

2.2.1 组织层面

燃气企业的信息安全组织力量薄弱且定位较低，企业没有形成自上而下的信息安全组织体系。

（1）企业信息化队伍并不完善，信息安全队伍严重匮乏，无法有效支撑企业的信息化建设和业务安全。

（2）企业对信息安全的认知度偏低，依然注重于传统的物理安全，并忽视信息安全问题与业务安全之间的重要性。

（3）企业各部门的信息安全职责不清，缺乏各部门和分子公司等单位的参与。

（4）缺乏信息安全的培训和意识提升机制，员工的信息安全意识薄弱。

（5）企业的信息化建设主要依赖于第三方，但是对第三方的管控薄弱且明显落后于信息化的建设速度。

2.2.2 策略层面

燃气企业基本没有成体系的信息安全策略，主要包括：

（1）事件驱动型，信息安全策略都是基于已发生的信息安全事件制定，缺乏体系化的制度流程支撑，信息安全策略侧重于应急响应机制。

（2）缺乏对信息系统和敏感信息的安全控制体系、技术规范以及安全基线。

（3）缺乏信息安全策略推广手段，信息安全策略难以落地实行。

（4）业务为先，较难平衡信息安全的控制以及业务效率之间的关系，信息安全策略要求更多“屈从”于业务要求。

（5）监督和考核机制不足，缺乏明确的策略要求，信息安全控制无法得到有效的落实。

2.2.3 技术层面

燃气企业已经部署基本的信息安全防护设施，如防火墙、入侵检测、流量监测等设施，但是存在以下问题：

（1）信息安全系统“孤岛”效应严重，无法形成有效合力。

（2）系统和网络的边界控制能力薄弱，不同的系统和网络间的资源访问控制颗粒度较粗，缺乏有效的监控和审计能力。

（3）企业业务复杂，第三方厂商技术水平参差不齐，安全技术能力薄弱。

（4）工控系统由于在网络中的互联性增加，导致多种途径可访问这些系统，从而导致更多潜在攻击的可能性。

（5）系统的建设和部署缺乏信息安全考虑，信息系统自身存在大量漏洞，这些问题极易被黑客所利用，严重影响到信息系统的运行安全。

2.3 燃气行业信息安全成熟度

越来越多的燃气企业高层管理人员认识到信息安全的重要性，但是无法了解企业自身信息安全所处的位置，不知道企业的信息安全未来发展之路如何走。参考信息安全控制最佳实践CoBIT[3]，可定义燃气企业信息安全成熟度级别为初始级、可重复级、已定义级、可管理级和已优化级5个级别。初始级指企业信息安全管理流程不存在，或信息安全工作流程缺乏统筹安排；可重复级指信息安全管理流程遵循固定的模式；已定义级指信息安全体系已建立标准化的书面程序；可管理级指信息安全体系流程可监控、可度量；已优化级指信息安全工作流程自动化且持续优化。

国内绝大部分燃气企业信息安全现状与北京燃气在进行信息安全体系建设之前的状况一样，处于第一级即初始级；燃气企业的信息安全要达到一定的程度则信息安全成熟度必然要达到持续优化的第4级，即

已管理级。通过信息安全成熟度模型，企业能够准确的找到当前所处的位置，未来企业信息安全期望达到的目标，以及企业未来信息安全的具体发展路线。

3 企业建立信息安全体系的思路和方法

3.1 传统信息安全管理存在的误区

为实现组织的信息安全，各厂商、各标准化组织都基于各自的角度提出了各种信息安全管理的体系标准，这些基于产品、技术与管理层面的标准在某些领域得到了很好的应用，但从组织信息安全的各个角度和整个生命周期来考察，现有的信息安全管理体系与标准是不够完备的，特别是忽略了组织中最活跃的因素——人的作用。

考察国内外的各种信息安全事件，发现在信息安全事件表象后面其实都是人的因素在起决定作用。不完备的安全体系是不能保证日趋复杂的组织信息系统安全性的。因此，组织为达到保护信息资产的目的，应在“以人为本”的基础上，充分利用等级保护、ISO27000、ISO20000、CoBIT等信息化控制标准与最佳实践，制定出周密的、系统的、适合组织自身需求的信息安全管理体系。

3.2 信息安全管理体系模型

信息安全的建设是一个系统工程，需要对信息系统的各个环节进行统一的考虑、规划和构架，并要时时兼顾组织内不断发生的变化，任何环节上的安全缺陷都会对系统构成威胁。

从宏观的角度来看，信息安全可以由以下HTP模型来描述：人员与管理（Human and management）、技术与产品（Technology and products）、流程与体系（Process and framework）。见图1。

图1 HTP——“以人为本”的信息安全模型

其中人是信息安全最活跃的因素，人的行为是信息安全保障最主要的方面。人特别是内部员工既可以是对信息系统的最大潜在威胁，也可以是最可靠的安全防线。统计结果表明，在所有的信息安全事故中，只有20%~30%是由于黑客入侵或其他外部原因造成的，70%~80%是由于内部员工的疏忽或有意泄密造成的。站在较高的层次上来看信息和网络安全的全貌就会发现安全问题实际上都是人的问题，单凭技术是无法实现从“最大威胁”到“最可靠防线”转变的。

以往的各种安全模型，其最大的缺陷是忽略了对人的因素的考虑，在信息安全问题上，要以人为本，人的因素比信息安全技术和产品的因素更重要。与人相关的安全问题涉及面很广，从国家的角度考虑有法律、法规、政策问题；从组织角度考虑有企业信息安全治理结构、安全方针政策程序、安全管理、安全教育与培训、组织文化、应急计划和业务持续性管理等问题；从个人角度来看有职业要求、个人隐私、行为学、心理学等问题。

在信息安全的技术防范措施上，可以综合采用商用密码、防火墙、防病毒、身份识别、网络隔离、可信服务、安全服务、备份恢复、PKI服务、取证、网络入侵陷阱、主动反击等多种技术与产品来保护信息系统安全，但不应把通过部署所有安全产品与技术而达到信息安全的零风险为目标，安全成本太高，安全也就失去其意义。组织实现信息安全应采用“适度防范”（Rightsizing）的原则，就是在风险评估的前提下，引入恰当的控制措施，使组织的风险降到可以接受的水平，保证组织业务的连续性和商业价值最大化就达到了安全的目的。

信息安全不是一个孤立静止的概念，信息安全是一个多层面、多因素的、综合的、动态的过程，管理学上的木桶原理能够很好的说明信息安全各个环节之间的作用。

一方面，如果组织凭着一时的需要，想当然去制定一些控制措施和引入某些技术产品，都难免存在挂一漏万、顾此失彼的问题，使得信息安全这只“木桶”出现若干“短木块”，从而无法提高安全水平。正确的做法是遵循信息安全标准与最佳实践过程，考虑组织对信息安全各个层面的实际需求，在风险分析的基础上引入恰当控制，建立合理安全管理体系，从

而保证组织赖以生存的信息资产的安全。

另一方面，这个安全体系还应当随着组织环境的变化、业务发展和信息技术提高而不断改进，不能一劳永逸，一成不变。因此，实现信息安全是一个需要一个完整的体系来保证的持续过程。

3.3 建立信息安全管理HTP体系的方法[4]

此方法论由国内著名的信息安全专家和IT治理专家陈伟提出，已被国内许多银行和央企采用。

3.3.1 HTP方法论框架

根据自顶向下，逐步求精的原则，根据组织的业务目标与安全要求，首先要在组织中建立信息安全治理结构，对信息安全做出制度保证；然后综合考察业务环境与IT环境，进行风险评估，做出信息安全计划，建立并运行信息安全管理体系，初步达到粗粒度的信息安全；在完整的信息安全管理体系之上，建立“人力防火墙”与“技术防火墙”,在细粒度上保证信息安全；实施阶段性的信息系统审计，在持续不断的改进过程中保证信息的安全性、完整性、可用性及有效性，从而建立一套完整的、健壮的信息安全防御体系。

3.3.2 建立HTP体系的步骤

（1）在充分理解组织业务目标、组织文件及信息安全的条件下，通过ISO13335风险分析方法，建立组织的信息安全基线（Security Baseline）,对组织的安全现状有一个清晰的了解，并可以为以后进行安全控制绩效分析提供一个评价基础。

（2）根据安全基线分析报告，制定组织信息安全计划，包括组织建设计划、预算计划和投资回报计划。

（3）按照ISO27000标准建立信息安全管理框架，完善粗粒度的信息安全过程。建立框架后，再通过这种细粒度的安全措施－“技术防火墙”和“人力防火墙”,就有可能建立起完备的信息安全管理体系。

（4）重视信息安全中最活跃的因素——“人”，建立“人力防火墙”，实现从信息安全“最大威胁”到 “最可靠防线”转变，这样才能真正调动组织中实现长治久安的内在动力。

（5）根据风险评估的结果，综合利用各种信息安全技术与产品，以“适度防范”为原则，建立有效的“技术防火墙”，这是实现信息安全管理的可靠外部保证措施。

（6）实施阶段性的信息系统审计，在持续不断的改进过程中保证信息安全性、完整性、可用性及有效性。

3.4 燃气行业信息安全体系建设方法

根据国内燃气行业信息安全的现状与特点，结合HTP信息安全体系建设方法论，下面提出燃气行业信息安全体系的建设方法。

3.4.1 燃气行业信息安全体系建设方法

图2 燃气行业信息安全体系建设方法

如图2所示。根据燃气企业的战略目标和风险现状，结合信息安全最佳实践，满足上级单位的监管要求，兼顾燃气企业生产安全和信息安全的结合点——工控安全，在确保外包服务安全的前提下设计燃气企业的信息安全架构，并综合燃气企业的战略目标和安全风险规划信息安全实施路线图，此蓝图作为未来信息安全体系建设的指南。

在此基础上考虑组织、制度、技术体系的建设，实现HTP理论中“人力防火墙”和“技术防火墙”的目标，先试点运行并最终全面推广，在此过程中应充分结合当前的环境推进信息安全意识教育，树立企业正确的信息安全文化。

在体系的建设和运行过程中应充分考虑企业的风险现状，不断提升和改进企业的风险管控措施，实现燃气企业的信息安全管理体系PDCA循序渐进的过程。在整个体系的设计、规划、建设以及运行过程中应保持各部门各单位之间的有效沟通和协调，保证体系的正常运行，并不断监控体系实施过程中的状况，

防止与业务目标的偏离，提升燃气企业信息安全体系的保障能力。

3.4.2 燃气行业信息安全体系建设步骤

燃气行业信息安全体系的建设建议按以下5个步骤进行：

（1）现状调研和风险评估；

（2）架构设计和蓝图规划；

（3）信息安全体系建设；

（4）信息安全意识培训；

（5）信息安全体系优化。

3.4.3 燃气行业信息安全架构设计

信息安全架构是对信息安全治理机制的高度概括，从信息安全目标和方针、信息安全策略，到信息安全管理工作的分解，再到信息安全管理工作如何开展，提出了方向性和原则性指导意见。

在信息安全架构（见图3）中，设置信息安全目标和信息安全方针作为安全架构的核心；为实现信息安全目标和方针，需要构建信息安全域，不同企业构建的信息安全域的情况可能会不一样；最后再通过3个体系来保证信息安全域的实施和落地。

在构建燃气行业的信息安全架构时应充分利用等级保护、ISO27000、ISO20000、CoBIT等信息化控制标准与最佳实践，制定出周密的、系统的、适合组织自身需求的信息安全架构。

燃气企业在构建信息安全架构时除了吸收最佳实践标准外，还应充分考虑风险评估、战略驱动以及监管要求等内容，最终将国际国内信息安全最佳实践标准裁剪成符合燃气企业的信息安全体系架构。

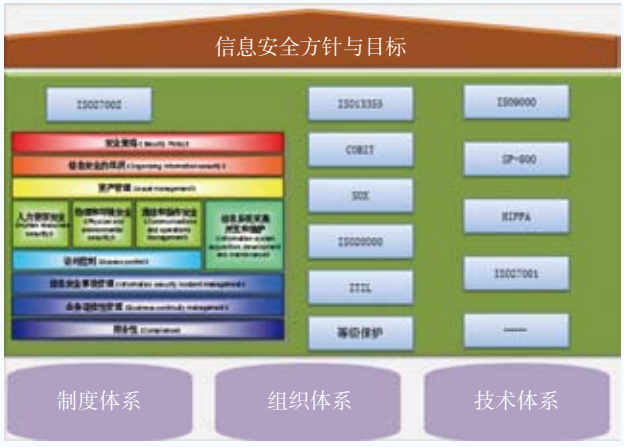

图3 燃气行业信息安全架构框架

3.4.4 燃气行业信息安全体系构建

燃气行业在信息安全体系的建设过程中为保障信息安全体系有效性，一般会遵从“组织体系定职责、策略体系定依据、技术体系定手段”的原则构建“事前防御、事中控制、事后响应”的信息安全体系，推进信息安全体系的执行和落地。

（1）组织体系

燃气企业应建立和完善信息安全决策、管理、执行以及监管的机构，明确企业所有单位的信息安全角色与职责以及总部和分公司之间的关系。信息安全组织体系处于信息安全战略的核心，是信息安全战略落实的基础和保障。

（2）策略体系

策略体系主要包含信息安全策略/方针、各信息安全管理域的安全管理要求等，为燃气企业提供信息安全控制依据。

（3）技术体系

燃气企业的信息安全技术体系应整合各种成熟的信息安全技术与产品，对企业各类信息资产形成有效的差异化和精细化保护。依据纵深防御的原则，结合“横向隔离，纵向认证”的要求，采用不同层次的防护技术，如身份认证、访问控制、内容安全、监控审计和备份恢复等，实现信息资产的安全防护。

4 北京燃气信息安全体系建设实践及应用

北京燃气集团于2012年10月份启动了信息安全体系建设项目，于2013年6月底结项。整个项目的建设基本遵循燃气行业信息安全体系建设方法，是对燃气行业信息安全体系建设方法的实践和应用，同时根据实践的结果再返回去对燃气行业信息安全体系的建设方法进行了完善。

4.1 建设目标

（1）通过现状调研和风险评估，全方位了解北京燃气信息安全工作现状和存在的风险。

（2）设计北京燃气的信息安全体系架构，完善信息安全组织与管理策略，编写信息安全制度与标准；并推进信息安全管理体系的落地运行。

（3）建立信息安全管理体系实施蓝图，使北京燃气能够利用3年到5年时间，建立起较为完善的信息

安全管理体系。

（4）培育一批具备信息安全专业水平的技术人员和管理人员，并全面提升员工的信息安全意识。

4.2 现状调研和风险评估

为全面梳理北京燃气信息系统安全现状，项目组对北京燃气信息化组织结构、物理环境安全、人力资源、信息资产、信息系统的开发和运行以及北京燃气各专业机构和分子公司的信息化建设和管理过程做了全面细致的了解，形成了北京燃气信息安全现状调研报告。

依据ISO27001国际标准，对北京燃气的信息安全现状进行了对标，查找与国际信息安全最佳实践之间的差距，并通过风险评估和分析进行分类和汇总，形成了包括应用系统风险、访问控制风险、外包服务风险、人员环境风险、组织安全风险等11个类别的风险。为将信息安全风险降低到北京燃气可以接受的水平，项目组为各类风险选择了恰当的风险处置措施并制定了从近期到长期详细的风险处置计划。

4.3 架构设计和蓝图规划

依据前期调研发现的问题和风险、遵照国际国内最佳实践标准、结合北京燃气的“十二五”规划设计完成了北京燃气的信息安全架构，并规划了北京燃气未来3年至5年的信息安全建设路线。

4.3.1 架构设计

北京燃气信息安全体系依照北京燃气信息安全整体目标，围绕“构建信息安全体系、保障信息系统安全”的方针制定了北京燃气的信息安全架构（如图4所示），通过组织体系定职责、制度体系定依据、技术体系定手段，涵盖了包括体系管控、建设安全、运维安全、应急保障和基础保障在内的五大信息安全域，全面覆盖北京燃气信息安全的各个方面。

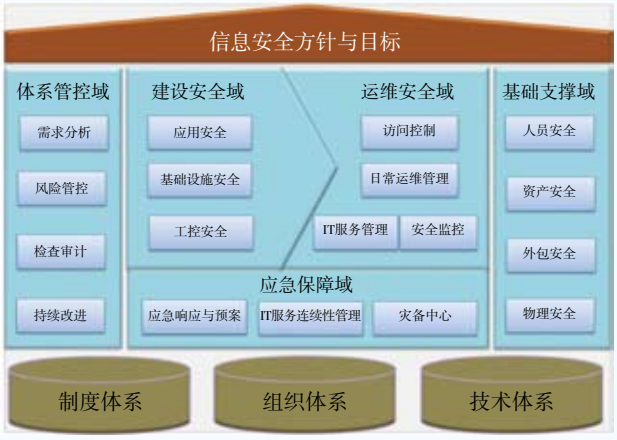

图4 北京燃气信息安全架构

北京燃气的五大信息安全域主要是参考ISO27001信息安全管理体系中的11个信息安全域，并结合燃气行业信息安全工作的特点和北京燃气已有的信息安全基础，重新进行划分和归并而得。

4.3.2 蓝图规划

信息安全蓝图规划目的是明确北京燃气未来信息安全的建设路线，经过3年乃至5年信息安全规划的实施，可以逐步改变目前信息安全的现状，为北京燃气信息系统的平稳运行和业务的持续开展提供强有力的保障。

北京燃气未来5年信息安全蓝图规划如下，分为以下3个阶段：

（1）信息安全管理体系建立阶段（2013年）。北京燃气于2013年上半年建立信息安全管理体系，通过信息安全管理体系的建设，建立了信息安全组织、完善了信息安全制度；通过持续进行风险评估，使北京燃气在信息安全方面具有了自我完善的能力。

（2）IT风险精细化管理阶段（2014年–2015年）。从2014年开始，进行IT综合管控体系的建设，建立完善的IT治理机制、IT综合管理流程（项目管理、外包管理、数据管理等）、IT服务管理流程、软件开发管理流程和IT绩效管理体系等；通过部署安全管理中心（SOC）开展敏感信息泄漏防护工作，试点关键用户信息安全绩效测评工作，推动信息安全工作的深入开展。

（3）安全与业务融合阶段（2016年–2017年）。从2016年开始，北京燃气的信息安全将进入安全与业务融合阶段，主要表现为，通过精细化信息安全管控体系的建立、IT内控体系建设，完善业务领域的信息安全工作，结合敏感信息防护工作的开展，实现安全与业务的深度融合，为IT支持业务运行与业务创新而奠定基础。

4.4 体系构建

4.4.1 组织保障体系

北京燃气的信息安全组织体系（见图5）包括领导层、管理层、执行层以及监督层。领导层由集团的信息化工作委员会担任。管理层由集团信息安全管理

小组担任，下设信息安全管理办公室，成员包括总部相关部门的信息安全协调员。执行层由信息档案中心、运营调度中心以及集团其他所属各单位组成。监督层由集团法审部和第三方审计机构组成。

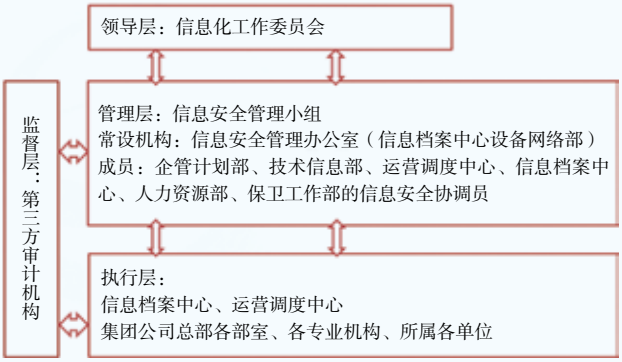

图5 北京燃气信息安全组织体系

通过信息安全组织体系的建立，明确了集团各属单位信息安全角色与职责，以及总部和分公司之间信息安全接口与互动关系。信息安全组织保障体系处于信息安全战略的核心，是信息安全战略落实的基础和保障，同时，信息安全制度保障体系的建立和执行、信息安全运行相关工作以及信息安全技术在北京燃气内的运用也需要信息安全组织保障体系相关机构和角色去具体落实。

4.4.2 制度保障体系

制度保障体系主要包含北京燃气的信息安全策略/方针、各信息安全管理域的安全管理规定、细则和表单类的文档，为北京燃气提供信息安全依据。在制度体系中明确了信息安全技术类各种标准、安全规范、配置基线等；制定了信息安全运行保障机制以及总部和分公司的信息安全协作机制。

目前制定的制度规范共32个，其中二级规定1个、三级办法6个、四级细则12个、技术规范13个，覆盖了系统建设、系统运行、应急保障、体系管控、基础保障五大领域。

4.4.3 技术保障体系

北京燃气建立了“五纵五横”的技术保障体系（见图6），实现从物理环境到终端数据的安全控制，建立了事前预防、事中监控以及事后恢复的相关机制。

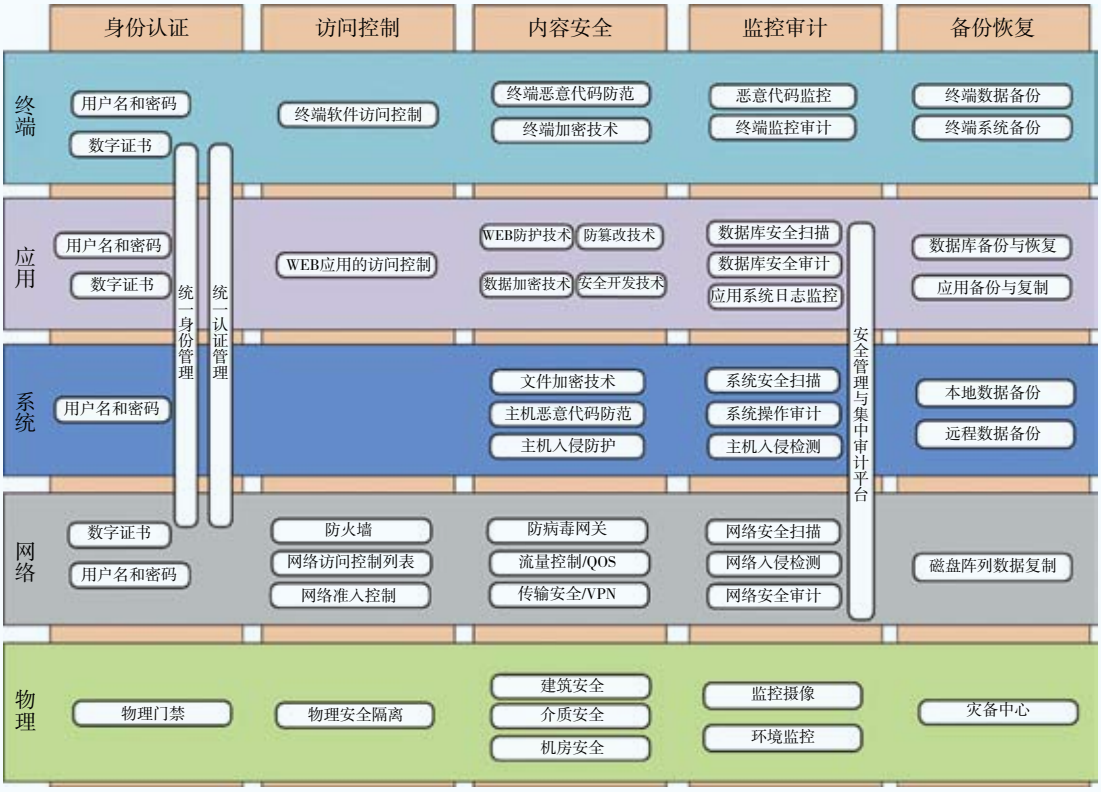

图6 北京燃气信息安全技术体系

北京燃气的技术保障体系将重点关注和解决：完善安全域的综合规划和整改、建立信息系统基本等级防护技术体系、建立PKI体系、建立4A平台、建立终端防护体系、建立信息安全监控体系和建立灾备中心。

4.5 信息安全意识的宣贯和提升

北京燃气在信息安全体系的建设过程中考虑了各个层面“人”的要素，从管理层到普通员工，从专业人员到非专业人员，充分保障了各层面人员所需的信息安全意识和技能的培养，如图7所示。

图7 北京燃气信息安全培训体系

在构建自身的信息安全宣贯体系的同时，考虑了自身企业文化和企业特点，在借助传统的宣传媒介的同时引入社会化媒体进行企业内部员工信息安全意识的宣传，建立多维度全方位的信息安全宣传渠道，如图8所示。

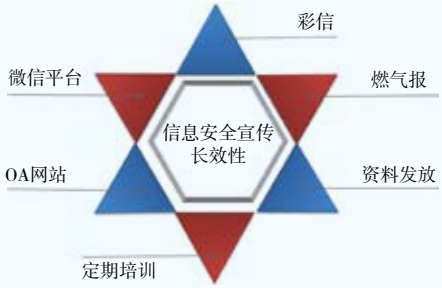

图8 北京燃气信息安全意识宣传渠道

5 燃气行业信息安全体系建设成功因素

信息安全风险是应用信息技术过程所必须面对的问题，因此建立信息安全体系是保障燃气企业业务和信息化持久发展的基础。结合北京燃气信息安全体系建设的过程和经验，总结几点燃气行业信息安全体系成功实施的要素：

（1）来自企业高层明确的支持和承诺，尤其对于相对传统的燃气行业而言这是信息安全体系有效推进的保障。

（2）注重体系落地，依据“总体规划、分步实施”的战略，信息安全体系建设要从全局的观念出发组建系统，制定具体的且可实现的计划。

（3）信息安全部门的定位问题以及与信息化之间的关系，明确信息安全与信息化是相互交叉又彼此区别的关系。

（4）加大信息安全的培训并建立自己的信息安全队伍，同时借助多种手段向所有管理者和员工有效的宣贯安全意识,注重持续性和时效性，减少信息安全在实施过程中的阻力。

（5）完善信息安全架构体系，增加信息安全纵深，整合现有信息安全设施，形成信息安全合力，避免不必要的资源浪费。

6 结束语

北京燃气的信息安全建设才刚刚起步，燃气行业其他企业的信息安全建设也即将开始，本文将在北京燃气信息安全体系建设过程中的经验、方法进行整理，在国内首次提出燃气行业的信息安全体系建设方法，供燃气行业其他企业构建信息安全体系参考。燃气企业信息安全的发展必然是不断变化和前进的过程，北京燃气比较注重信息安全体系建设落地的实际效果，不断夯实信息安全的基础，关注信息安全未来的发展方向，持续优化已建立的信息安全体系架构，使之符合燃气企业自身的安全需求并保障燃气业务的安全运行。

参考文献

1 欧洲网络与信息安全局ENISA，2012年威胁报告

2 CoBIT 4.1 ISACA

3 陈伟. 企业建立信息安全管理体系的思路与方法. 北京燃气报信息安全专刊，2013；6

4 北京燃气信息安全体系建设项目技术方案