doi:10.3969/j.issn.1671-5152.2013.05.010

浅析燃气企业的信息安全管理

□　镇江华润燃气有限公司（212009）周　滨

摘　　要： 针对燃气企业存在的信息安全问题，本文试图通过PDCA的理论方法，体系化的从规划、实施、检查、处置4个步骤，循环推进企业信息安全建设。并提出要特别重视解决风险评估、人的角色和职责、信息资产管理、信息安全事件管理等关键环节来保障企业信息安全建设有效实施。

关 键 词： 信息安全　风险评估　管理　燃气

Information Security Management of Gas Enterprises

Zhenjiang China Resources Gas Co.,Ltd（212009）Zhou Bin

Abstract: Aiming at solving the problems of information security system of gas enterprises, this paper attempts to use PDCA theory and its methods and through four steps of Planning, Doing, Checking and Acting to promote the construction of enterprise information security. It also pays high attention to the key links of addressing risk assessments, the personal roles and responsibilities, the management of information assets and the management information security incidents and puts forward ways to ensure the effective implementation of enterprise information security.

Keywords: information security　risk assessment　management　gas

如今，信息已成为企业生产和发展的重要资源之一。它以多种形式存在，如被打印或写在纸上；以电子方式存储；用邮寄或电子手段传送；呈现在胶片上或用语言表达。无论信息以什么形式存在，用哪种方法存储或共享，都应对它进行适当地保护。否则，企业将面临着较大的信息安全风险，甚至给企业带来不

突出，群众是否满意”等5个方面，结合企业生产和服务的实际，建立完善考核机制，不断深化具有燃气特色的“轻轻松松做不了共产党员”主题实践活动，动员每个党员积极投身“为民务实清廉”为主题的党的群众路线教育实践活动中，贴近群众，脚踏实地、求真务实，用服务群众的实际行动证明自己的纯洁性、先进性和模范引领作用，在奉献中履行自己的真情誓言，在发展中树立党员的先锋形象，最大程度地发挥党员的先进性，为打造与世界石油城相适应的一流燃气公司，为建设美丽克拉玛依而努力。

良的影响和后果。

1 燃气企业管理存在的信息安全问题

信息安全问题是企业的共性问题，企业规模越大，所拥有价值的信息量就越大；企业经营性质越特殊，受保护的信息量就越多。燃气企业是高危服务性行业，应当把燃气运营安全放在首位，但是也不能忽视了企业的信息安全。信息安全问题在燃气企业普遍存在。

1.1 缺乏系统的信息安全管理

网络安全领域有一句至理名言“三分技术，七分管理”，这句话对于信息安全领域也同样适用。安全与管理常常是密不可分的，很多企业对信息安全的认识仅仅是依靠信息防护技术应用，比如安装防火墙，反病毒软件等。但信息软件技术只是信息安全的一部分，即便在安全设备与系统上做了很大的投入，缺乏完整、系统的安全管理方法及制度并贯彻实施，信息仍然得不到很好的保护。尤其是那些对于针对黑客攻击还显得相对脆弱的企业网络，一旦遭遇恶意入侵，马上便显得不堪一击，信息安全当然就完全谈不上。而现实情况是，许多燃气企业因为缺乏信息安全管理制度、方法和应急预案，对于这种情况全然没有有效的防备和事后补救措施，这样灾难自然就是难免的了。

1.2 信息安全意识有待提高

当前，企业的信息载体日益电子化，信息系统、办公电脑、移动存储设备的不规范使用增加了电子信息的泄露发生率。在百度、谷歌、网络文库上稍加搜索就可以轻易的获得某家燃气集团或公司重要文件。这些重要信息资料被暴露在公众中，正是由于燃气企业以及员工信息安全意识不强所造成的。而不少企业的领导者对于重要信息的保护意识不强，尤其是企业员工，从思想上就不重视企业的信息安全，信息传递和交接都带有很大的随意性，更有些“大嘴巴”事件，使得企业许多重要信息外流，如客户信息、企业内部信息，更有甚者，许多商业机密也轻易外泄，如燃气危险源信息或燃气成本等。

1.3 缺乏信息安全技术人才

在燃气企业，由于对企业信息安全的重要性认识不足，普遍缺乏信息安全管理人员和信息系统安全技术人员。虽然近年来燃气企业各类信息系统不断增多，如地理信息系统、客户服务系统、数据采集与监视控制系统等，涌现出了一批信息化技术人才，但是要从安全角度出发，能够进行综合信息安全管理的技术性人才在整个燃气企业员工的比例仍然相当低。燃气企业在信息安全人才和信息技术人才培养方面与企业快速发展带来的信息化需求和信息安全需求显然不能同步，这样一来，对于信息外泄，信息安全防不胜防，便会出现“领导干瞪眼，群众干着急”的局面。

2 理解信息安全的基本内容和信息安全建设的主要任务

2.1 什么是信息安全?

在GB/T22081–2008中，信息安全被这样定义：保护信息免受各种威胁的损害，以确保业务连续性、业务风险最小化、投资回报和商业机遇最大化。其主要是指在企业信息安全管理中首先要最大限度的保护企业信息资产，保障业务持续稳定运行，其次，一旦发生安全事故可以最大限度地挽回所造成的损失。

信息的安全风险主要来自于信息的保密性、完整性和可用性。在企业中，信息可能会通过口头、网络、打印机、复印机、存储设备等途径不经意地泄露。要避免重要信息的泄露，在信息的传递和保管过程中要把好关；然后，还要防止信息被误变更或被恶意变更，做到保护信息的完整性；最后，要做好信息源头的安全保障，即要保障信息处理设备和信息传递渠道的高可用性。制定清晰的信息处理流程，建立满足服务的完善运维保障，以及设法保持业务连续性管理都是保证信息高可用的重要措施。正是信息的这3个属性结合才形成了信息的安全性，如图1所示：

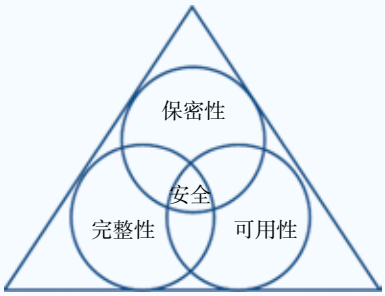

图1 安全属性

2.2 信息安全建设的主要工作任务应由以下几方面构成

即体系化的企业信息建设，信息安全风险控制和确保企业信息的机密性、完整性和可用性。而对于不少燃气企业来说，却常常是重视了第1点，而忽略第2和第3点。因此，有计划的解决企业存在的信息安全风险，以及可持续提高管理的有效性和不断提高自身的信息安全管理水平是企业的当务之急。

3 采用PDCA循环的方法建设企业信息安全

作为一项安全管理活动，信息安全建设应该是符合一般管理活动的规律的。所以，用PDCA管理模式，即规划（Plan）实施（Do）检查（Check）处置（Act）的循环管理模式来指导燃气企业信息安全建设十分必要也非常合适。

PDCA的概念最早由美国质量管理专家戴明提出来，起初用于质量管理，后逐渐应用于各行各业。通过PDCA方法管理能使信息安全建设有效的按照一种合乎逻辑的工作程序进行。对其具体应用，笔者结合自己所学的理论知识和工作经验进行了总结。

3.1 P阶段

（1）分析公司信息管理中存在的不安全因素，采用合理的风险评估方法，确定风险并对风险进行分级；

（2）找出不安全因素产生的原因，特别是在企业管理层面上存在原因和需要企业高层处理的问题；

（3）针对存在的问题，根据风险等级对存在的隐患制订措施计划和解决方案，制定的措施方案要有较强的可操作性，便于执行，并能收到较好的效果。对于整改资金必须从安全与生产发展的总体考虑，结合实际，因地制宜，合理投入。

3.2 D阶段

（1）对风险整改计划进行宣贯和指导，让企业员工认识到存在的安全现状和不安全因素，以及怎样去改进。计划要落实到人，整改的人要清楚的理解为什么要改进和怎样改进；

（2）层层细化风险改进计划，并与员工的工作实际相结合。计划可以从企业管理层开始细化直至岗位上的每一个操作环节。如果细化不彻底，那么企业的总计划中的方案措施再有可操作性，相对于班组、岗位都存在不同程度的粗放性，很难与基层实际吻合。

3.3 C阶段

（1）开展企业各层级员工对自己工作进展情况的自查，查找问题，分析原因，及时整改；

（2）开展信息安全专项检查，定期和不定期检查风险改进的执行情况，阶段性的总结和考评执行效果。检查最好能通过量化式检查得出定性结论。这一方法的最大优点就是对每一个PDCA循环层进行横向比较时，能得到较为准确的评价，找准薄弱点和工作漏洞；

（3）对检查结果和现存信息风险重新进行总结和评估，并根据评估结果调整风险级别和风险值，找出重点关注环节。

3.4 A阶段

（1）统计汇总信息安全风险控制的成果，去除已经解决的问题，制订对新问题的改进计划；

（2）分清计划未完成的原因并确立相关责任人，依据有关规定进行严考核硬兑现；

（3）把遗留和新发现问题转入下一个PDCA管理

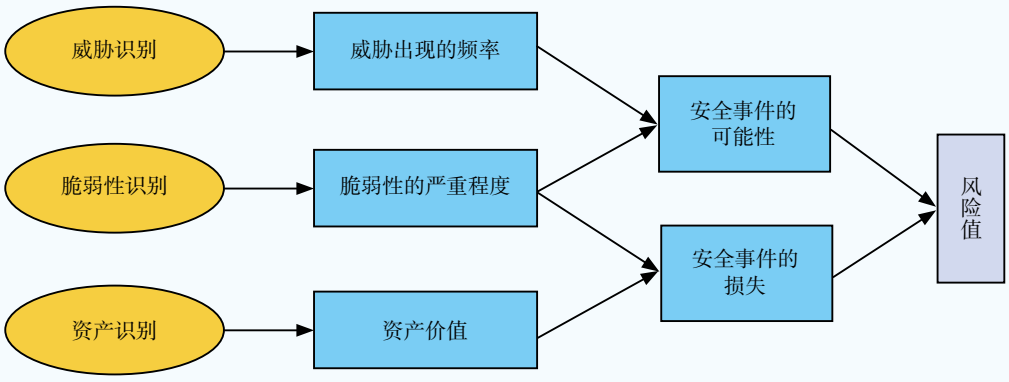

图2　风险评估

循环。

4 重点解决信息安全建设中的几个关键问题

4.1 把握风险评估尺寸，正确处理存在的风险

风险评估的实施方法有许多，在做信息安全风险评估时，应从企业整体出发，从企业需求出发。通过《信息安全技术信息安全风险评估规范》（GB/T20984–2007）给出的风险评估实施流程可以较为全面评估出企业存在的信息安全风险。

信息安全风险识别出后，采用合理的处置办法也非常重要。采用的处理方式主要有：①风险减缓，即采用适当的控制措施来降低风险。如对重要信息处理设备采用冗余配置措施以避免单点故障的发生；②风险接受，在明显满足组织方针策略和接受风险准则的条件下，有意识地、客观地接受风险。特别是适当接受那些“风险级别低的风险”，以确保高级别风险能及时而有效地处置；③风险规避，在可能的情况下，避免某些特殊风险，如将重要信息文件进行加密来避免未授权人获得；④风险转移，将相关业务风险转移到其它地方，如将网站业务的维护托管到第三方专业维保单位管理，并与其签订信息安全保密协议等。

4.2 重视人在燃气企业信息安全管理中的作用

在企业管理中，所有的管理活动离不开“人”。“人”是信息安全活动中最复杂、最难控制的对象，许多信息安全事件的发生是由人而起。要对企业中人的行为进行约束，明确人的信息安全管理角色和管理职责；加强人的思想认识，进行信息安全的教育和培训，才能构建良好的信息安全文化。

笔者所在公司在信息安全管理中，首先成立了信息安全小组，把企业的 “一把手”作为推动信息安全的组长，把企业内不同部门的人作为参与信息安全管理的对象，其中经理层和关键岗位人员是安全小组组员，明确了组长和组员的信息安全责任和义务；然后把信息安全责任制落实到企业安全责任状中，要求层层签订层层落实，通过与经理层、关键岗位人员签订保密承诺书，来进一步保障企业信息安全；最后注重培育企业自己的信息安全文化，特别是通过报纸、宣传栏、企业OA 系统向员工宣传日常信息安全做法，从小事出发将注重信息安全形成习惯。例如，对电子文件进行简单加密，离开电脑时进行锁屏保护、给电脑打开设定密码保护、重要文件不被设为共享，不把公司的文件传送给第三方（其它公司、网上文库），及时粉碎重要纸质文件，及时做好重要数据备份，及时更新杀毒软件病毒库等。

4.3 做好信息资产分类，把资产管理好

信息是一种对燃气企业具有价值的资产，但是要想把这种资产管好，必须做到以下几点：第一，它有两种存在形式，即有形和无形，要建立信息资产清单来管理，这样在管理中才能做到“胸中有数”；第二，不同信息有着不同保护要求，要进行信息分类管理，根据不同分类等级采取不同的保护措施。信息保护等级可分为：绝密、机密、秘密、受限、内部公开、公开。在分类时特别要注意的是考虑共享或限制信息的业务需求以及与这种需求相关的业务影响，避免信息保护等级被设定过高，实际操作时影响到业务的开展；第三，信息的处理过程很难控制，需要对信息做好标记，标记的内容要包括安全处理、存储、传输、删除、销毁的处理程序，标记的程序要涵盖物理和电子格式的信息资产，不能有遗漏。特别是对报废的存储介质处理，应确保销毁，因为以目前的数据恢复技术而言，采用格式化的方法来处理数据存储的物理介质很容易被恢复。因此，最好的办法是物理销毁、数据覆盖或者利用不可逆专门工具处理。

4.4 合理规划信息安全区域，做好信息处理设备的安全管理

在燃气安全生产建设中分清防爆区域非常重要，其实信息安全管理中也要分清信息安全区域，通常在实际应用中将总经理室、财务部门、人力资源部门、档案部门、图纸设计部门、信息化部门、信息系统机房等具有敏感信息的部门划定在安全区域内，并在物理边界上加以防护，防止未授权的人员进入损坏、盗窃、截取。如在财务部门、信息化机房入口安装门禁、视频监控、围栏、红外报警器等。

此外，还要考虑安全区域内的信息安全。笔者发现在日常工作中设备故障所造成的信息处理过程不安全最为常见。因此，对提供信息处理支持性设施要格外关注，要加强设施的运维管理，建立运维管理制度，安排专人定期巡检设备运行情况。条件允许下，还可以配置冗余的硬件设备，双回路的供电电源，应

急电源等。

4.5　加强信息安全事件管理，预防信息安全事件发生

据燃气企业发生的各种信息安全事件的统计结果，最典型的有有害程序、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件等。其中，带来的损失最严重的是有害程序、网络攻击事件。针对这些事件，可以采取相应的技术防范措施，如安装反病毒产品、防火墙产品、入侵检测与入侵防御产品，对系统和网络进行脆弱性扫描等，同时做好定期设备的巡查，及时更换失效的产品。

另一方面，根据本企业自身情况建立信息安全应急预案，搭建应急组织机构，对信息安全事件分级，并制定应急响应机制、应急处置流程（即事故上报流程）以及恢复程序。每年开展一次应急演练，提高信息安全应急预案的可操作性以及相关人员对信息安全事件响应的熟练程度，可以提高信息安全事件的预防和处置能力。

5　未来持续性做好信息安全工作的几点探索

“发展”和“变化”始终是未来信息安全的重要特征，只有紧紧抓住这个特征才能正确地处理和对待信息安全问题。笔者认为燃气企业未来应从如下两个方面持续做好信息安全管理。

5.1　正确面对新技术的应用

随着无线技术、物联网技术、“云”技术等新技术在企业中应用，企业在信息应用上取得很大突破，新的信息技术为企业发展带来了新的机遇。但是不断革新的技术就像一把“双刃剑”，一方面它促成了企业的新发展，而另一方面也会为企业带来新的信息安全问题。因此，企业应正确的面对新技术，在新技术应用同时，重视加强入侵检测技术、RFID（射频识别）技术、数字认证加密技术、灾难备份技术等安全防护技术的应用，以保障企业在新形势下的信息安全。与此同时，通过实践我们也应该提高防范意识，谨防别有用心之人利用信息新技术来造成信息破坏或信息安全事故。

5.2　大力发挥人才的优势

信息安全管理离不开人，信息技术的应用和维护更离不开人。笔者认为持续性做好信息安全管理的另一突破点在人才管理上。燃气企业应着力培养一批懂信息技术、懂安全、懂燃气的综合性人才，大力发挥人才优势，才能使得信息安全保护持续性得到有力支撑。

参考文献

1 GB/T22080–2008 信息技术 安全技术 信息安全管理体系 要求

2 GB/T22081–2008 信息技术 安全技术 信息安全管理实用规则

3 GB/T20984–2007 信息安全技术 信息安全风险评估规范

工程信息

2013年牡丹江市将投巨资实现天然气管网过江

2013年3月21日了解到，牡丹江中燃城市燃气发展有限公司将投资4 000万元在江南新区新建两座CNG加气站，投资1 200万元实现天然气管网过江，投资600万元新建安装3 000余个天然气用气户。

据了解，牡丹江市江南新区2012年末建立天然气江南LNG（液化天然气）站，开通了管道天然气，截至2013年3月20日已安全运行3个月，每天用气量约500m³，累计输送天然气4.3万余m³。目前，江南新区已经铺设天然气中压管线10.54km，庭院管线3.8km，投入使用居民小区调压站2座，现已对环龙湾、塞纳丽舍、百好花园3个较大的居民小区输送了环保清洁的管道天然气，用气居民超过5 000户。

（本刊通讯员供稿）